PX2-3000/4000/5000 Series

User Guide
Release 2.4

Copyright © 2013 Raritan, Inc.

DPX2-0H-v2.4-E

February 2013

255-80-6101-00

Safety Guidelines

WARNING! Read and understand all sections in this guide before installing or operating this product.

WARNING! Connect this product to an AC power source whose voltage is within the range specified on the product's nameplate. Operating this product outside the nameplate voltage range may result in electric shock, fire, personal injury and death.

WARNING! Connect this product to an AC power source that is current limited by a suitably rated fuse or circuit breaker in accordance with national and local electrical codes. Operating this product without proper current limiting may result in electric shock, fire, personal injury and death.

WARNING! Connect this product to a protective earth ground. Never use a "ground lift adaptor" between the product's plug and the wall receptacle. Failure to connect to a protective earth ground may result in electric shock, fire, personal injury and death.

WARNING! This product contains no user serviceable parts. Do not open, alter or disassemble this product. All servicing must be performed by qualified personnel. Disconnect power before servicing this product. Failure to comply with this warning may result in electric shock, personal injury and death.

WARNING! Use this product in a dry location. Failure to use this product in a dry location may result in electric shock, personal injury and death.

WARNING! Do not rely on this product's receptacle lamps, receptacle relay switches or any other receptacle power on/off indicator to determine whether power is being supplied to a receptacle. Unplug a device connected to this product before performing repair, maintenance or service on the device. Failure to unplug a device before servicing it may result in electric shock, fire, personal injury and death.

WARNING! Only use this product to power information technology equipment that has a UL/IEC 60950-1 or equivalent rating. Attempting to power non-rated devices may result in electric shock, fire, personal injury and death.

WARNING! Do not use a Raritan product containing outlet relays to power large inductive loads such as motors or compressors. Attempting to power a large inductive load may result in damage to the relay.

WARNING! Do not use this product to power critical patient care equipment, fire or smoke alarm systems. Use of this product to power such equipment may result in personal injury and death.

WARNING! If this product is a model that requires assembly of its line cord or plug, all such assembly must be performed by a licensed electrician and the line cord or plugs used must be suitably rated based on the product's nameplate ratings and national and local electrical codes. Assembly by unlicensed electricians or failure to use suitably rated line cords or plugs may result in electric shock, fire, personal injury or death.

WARNING! This product contains a chemical known to the State of California to cause cancer, birth defects, or other reproductive harm.

Safety Instructions

1. Installation of this product should only be performed by a person who has knowledge and experience with electric power.
2. Make sure the line cord is disconnected from power before physically mounting or moving the location of this product.
3. This product is designed to be used within an electronic equipment rack. The metal case of this product is electrically bonded to the line cord ground wire. A threaded grounding point on the case may be used as an additional means of protectively grounding this product and the rack.
4. Examine the branch circuit receptacle that will supply electric power to this product. Make sure the receptacle’s power lines, neutral and protective earth ground pins are wired correctly and are the correct voltage and phase. Make sure the branch circuit receptacle is protected by a suitably rated fuse or circuit breaker.
5. If the product is a model that contains receptacles that can be switched on/off, electric power may still be present at a receptacle even when it is switched off.

This document contains proprietary information that is protected by copyright. All rights reserved. No part of this document may be photocopied, reproduced, or translated into another language without express prior written consent of Raritan, Inc.

© Copyright 2013 Raritan, Inc. All third-party software and hardware mentioned in this document are registered trademarks or trademarks of and are the property of their respective holders.

FCC Information

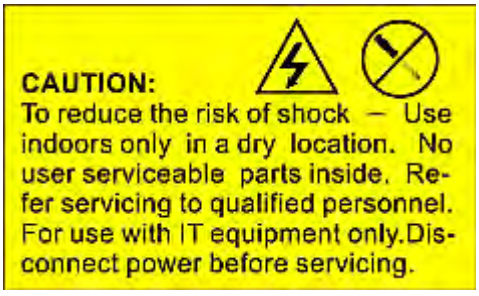
This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial installation. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. Operation of this equipment in a residential environment may cause harmful interference.

VCCI Information (Japan)

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Raritan is not responsible for damage to this product resulting from accident, disaster, misuse, abuse, non-Raritan modification of the product, or other events outside of Raritan's reasonable control or not arising under normal operating conditions.

If a power cable is included with this product, it must be used exclusively for this product.


CAUTION:
To reduce the risk of shock – Use indoors only in a dry location. No user serviceable parts inside. Refer servicing to qualified personnel. For use with IT equipment only.Disconnect power before servicing.

Contents

Safety Guidelines ii

Safety Instructions iii

Applicable Models xiv

What's New in the PX User Guide xvi

Chapter 1 Introduction 1

Product Models 1
Product Features 1
Package Contents 4
Zero U Products 4
1U Products 4
2U Products 4

Chapter 2 Rack-Mounting the PDU 5

Rackmount Safety Guidelines 5
Circuit Breaker Orientation Limitation 5
Mounting Zero U Models Using L-Brackets 6
Mounting Zero U Models Using Button Mount 7
Mounting Zero U Models Using Claw-Foot Brackets 9
Mounting Zero U Models Using Two Rear Buttons 10
Mounting 1U or 2U Models 11

Chapter 3 Installation and Configuration 13

Before You Begin 13
Unpacking the Product and Components 13
Preparing the Installation Site 13

Checking the Branch Circuit Rating....14
Filling Out the Equipment Setup Worksheet....14
Installing Cable Retention Clips on the Inlet (Optional)....14
Connecting the PDU to a Power Source....15
Configuring the PX....16
Connecting the PX to a Computer....17
Installing the USB-to-Serial Driver (Optional)....18
Connecting the PX to Your Network....20
Initial Network Configuration....22
Cascading the PX via USB....29
Installing Cable Retention Clips on Outlets (Optional)....31

Chapter 4 Connecting External Equipment 33

Connecting Environmental Sensors (Optional)....33
Contact Closure Sensors....35
Floor Water Sensors....43
Differential Air Pressure Sensors....46
Connecting the Asset Management Sensor (Optional)....47
Combining Asset Sensors....47
Connecting Asset Sensors to the PX....49
Connecting Blade Extension Strips....51
Connecting AMS-M2-Z Asset Sensors (Optional)....54
Using an X Cable....56
Connecting a Logitech Webcam (Optional)....58
Connecting a GSM Modem (Optional)....59
Connecting a Schroff LHX Heat Exchanger (Optional)....59
Connecting an RF Code PDU Sensor Tag (Optional)....60

Chapter 5 Using the PDU 61

Panel Components....61
Power Cord....61
Outlets....61
Connection Ports....63
LED Display....65
Reset Button....70
Circuit Breakers....71
Resetting the Button-Type Circuit Breaker....71
Resetting the Handle-Type Circuit Breaker....72
Fuse....73
Fuse Replacement on Zero U Models....73
Fuse Replacement on 1U Models....74

Beeper 76

Chapter 6 Using the Web Interface 77

Supported Web Browsers 77
Logging in to the Web Interface 78
Login 78
Changing Your Password 80
Logout 80
Introduction to the Web Interface 81
Menus 82
Dominion PX Explorer Pane 82
Setup Button 85
Status Bar 86
Add Page Icon 87
Logout Button 88
Data Pane 88
More Information 88
Viewing the Dashboard 93
Alerted Sensors 93
Device Management 94
Displaying the PDU Information 94
Naming the PDU 98
Modifying the Network Configuration 98
Modifying the Network Service Settings 105
Setting the Date and Time 110
Setting Up Default Measurement Units 112
Configuring the Feature Port 113
Configuring the Serial Port 114
Specifying the Device Altitude 115
Setting Data Logging 116
Configuring the SMTP Settings 117
Setting the EnergyWise Configuration 118
Rebooting the PX Device 119
User Management 119
Creating a User Profile 120
Modifying a User Profile 123
Deleting a User Profile 124
Changing the User List View 124
Setting Up Your Preferred Measurement Units 124
Setting Up Roles 125
Creating a Role 125
Modifying a Role 126
Deleting a Role 127
Changing the Role List View 128
Access Security Control 128
Forcing HTTPS Encryption 128
Configuring the Firewall 128
Setting Up User Login Controls 134
Setting Up Role-Based Access Control Rules 138

Setting Up an SSL Certificate 142
Certificate Signing Request 143
Creating a Self-Signed Certificate 145
Installing Existing Key and Certificate Files 146
Downloading Key and Certificate Files 147
Setting Up External Authentication 147
Gathering the External Authentication Information 148
Adding Authentication Servers 149
Sorting the Access Order 153
Testing the Server Connection 153
Editing the Authentication Server Settings 153
Deleting the Authentication Server Settings 154
Disabling External Authentication 154
Enabling External and Local Authentication Services 155
Outlet Management 155
Naming Outlets 155
Outlet Monitoring 156
Outlet Switching 158
Setting the Default Outlet State 160
Changing the Cycling Power-Off Period 161
Setting the Initialization Delay 164
Setting the Inrush Guard Delay 165
Setting the Outlet Power-On Sequence 165
Setting the Outlet-Specific Power-On Delay 166
Setting Non-Critical Outlets and Load Shedding Mode 167
Inlet and Circuit Breaker Management 170
Naming the Inlet 170
Naming Circuit Breakers 170
Monitoring the Inlet 171
Monitoring Circuit Breakers 172
Setting Power Thresholds 173
Setting an Outlet's Thresholds 173
Bulk Configuration for Outlet Thresholds 174
Setting Inlet Thresholds 175
Setting a Circuit Breaker's Thresholds 176
Bulk Configuration for Circuit Breaker Thresholds 177
What is Deassertion Hysteresis? 178
What is Assertion Timeout? 179
Event Rules and Actions 180
Components of an Event Rule 180
Creating an Event Rule 180
Sample Event Rules 208
A Note about Infinite Loop 211
Modifying an Event Rule 213
Modifying an Action 214
Deleting an Event Rule or Action 214
A Note about Untriggered Rules 215
Managing Event Logging 215
Viewing the Local Event Log 215
Clearing Event Entries 216

Viewing Connected Users 216
Monitoring Server Accessibility 217
Adding IT Devices for Ping Monitoring 217
Editing Ping Monitoring Settings 220
Deleting Ping Monitoring Settings 220
Checking Server Monitoring States 221
Environmental Sensors 221
Identifying Environmental Sensors 222
Managing Environmental Sensors 223
Configuring Environmental Sensors 224
Viewing Sensor Data 228
Unmanaging Environmental Sensors 232
Asset Management 232
Configuring the Asset Sensor 233
Setting Asset Sensor LED Colors 234
Configuring a Specific Rack Unit 235
Expanding a Blade Extension Strip 236
Displaying the Asset Sensor Information 237
Bulk Configuration 238
Saving a PX Configuration 239
Copying a PX Configuration 240
Backup and Restore of PX Device Settings 240
Webcam Management 242
Configuring Webcams 242
Adjusting Snapshot or Video Properties 243
Viewing the Webcam Snapshots or Videos 243
Sending Snapshots or Videos in an Email or Instant Message 244
Snapshot Storage 245
Network Diagnostics 248
Pinging a Host 248
Tracing the Network Route 248
Listing TCP Connections 249
Viewing the Communication Log 249
Downloading Diagnostic Information 250
Managing the Schroff LHX Heat Exchanger 251
Enabling and Disabling Schroff LHX Heat Exchanger Support 252
Configuring the LHX Device 252
Monitoring the LHX Device 254
Turning the LHX On or Off 257
Requesting Maximum Cooling for an LHX 257
Firmware Upgrade 258
Updating the PX Firmware 258
Viewing Firmware Update History 260
Full Disaster Recovery 260
Updating the Asset Sensor Firmware 261
Accessing the Help 261
Retrieving Software Packages Information 261
Browsing through the Online Help 261

Chapter 7 Using SNMP 263

Enabling SNMP....263
Configuring Users for Encrypted SNMP v3....264
Configuring SNMP Notifications....265
SNMPv2c Notifications....266
SNMPv3 Notifications....267
SNMP Gets and Sets....269
The PX MIB....270
Retrieving Energy Usage....272
A Note about Enabling Thresholds....272

Chapter 8 Using the Command Line Interface 273

About the Interface....273
Logging in to CLI....274
With HyperTerminal....274
With SSH or Telnet....275
Different CLI Modes and Prompts....276
Closing a Local Connection....276
Help Command....277
Querying Available Parameters for a Command....278
Showing Information....279
Network Configuration....279
PDU Configuration....281
Outlet Information....282
Inlet Information....283
Circuit Breaker Information....284
Date and Time Settings....284
Default Measurement Units....285
Environmental Sensor Information....286
Outlet Sensor Threshold Information....287
Outlet Pole Sensor Threshold Information....288
Inlet Sensor Threshold Information....289
Inlet Pole Sensor Threshold Information....290
Circuit Breaker Sensor Threshold Information....291
Environmental Sensor Threshold Information....293
Security Settings....294
Existing User Profiles....295
Existing Roles....296
Load Shedding Settings....296
Serial Port Settings....297
EnergyWise Settings....297
Asset Sensor Settings....297
Rack Unit Settings of an Asset Sensor....298
Blade Extension Strip Settings....299
Event Log....300
Command History....301

History Buffer Length 301
Reliability Data 302
Reliability Error Log 302
Examples 302
Clearing Information 304
Clearing Event Log 304
Configuring the PX Device and Network 305
Entering the Configuration Mode 305
PDU Configuration Commands 305
Networking Configuration Commands 314
Time Configuration Commands 339
Security Configuration Commands 343
Outlet Configuration Commands 366
Inlet Configuration Commands 368
Circuit Breaker Configuration Commands 369
Environmental Sensor Configuration Commands 370
Sensor Threshold Configuration Commands 374
User Configuration Commands 404
Role Configuration Commands 417
EnergyWise Configuration Commands 423
Asset Management Commands 425
Serial Port Configuration Commands 433
Setting the History Buffer Length 434
Multi-Command Syntax 435
Quitting the Configuration Mode 436
Load Shedding Configuration Commands 437
Enabling or Disabling Load Shedding 437
Power Control Operations 438
Turning On the Outlet(s) 438
Turning Off the Outlet(s) 439
Power Cycling the Outlet(s) 440
Unblocking a User 441
Resetting the PX 442
Restarting the PDU 442
Resetting to Factory Defaults 442
Network Troubleshooting 442
Entering the Diagnostic Mode 443
Diagnostic Commands 443
Quitting the Diagnostic Mode 446
Retrieving Previous Commands 446
Automatically Completing a Command 446
Logging out of CLI 447

Chapter 9 In-Line Monitors 448

Overview 448
Safety Instructions 448
Flexible Cord Installation Instructions 449
Flexible Cord Selection 449
Plug Selection 450

Receptacle Selection 450
Derating a Raritan Product 450
Wiring of 3-Phase In-Line Monitors 451
In-Line Monitor Unused Channels 451
Step by Step Flexible Cord Installation 451
In-Line Monitor's LED Display 456
Automatic Mode 456
Manual Mode 457
In-Line Monitor's Web Interface 457
Dashboard Page 458
Outlet Page 458

Appendix A Specifications 460

Power Measurement Accuracy 460
Maximum Ambient Operating Temperature 460
Serial RS-232 Port Pinouts 461
Sensor RJ-12 Port Pinouts 461
Feature RJ-45 Port Pinouts 461

Appendix B Equipment Setup Worksheet 463

Appendix C Resetting to Factory Defaults 467

Using the Reset Button 467
Using the CLI Command 468

Appendix D LDAP Configuration Illustration 470

Step A. Determine User Accounts and Groups 470
Step B. Configure User Groups on the AD Server 471
Step C. Configure LDAP Authentication on the PX Device 472
Step D. Configure User Groups on the PX Device 474

Appendix E Integration 478

Power IQ Configuration 478
Adding PDUs to Power IQ Management 478
Dominion KX II Configuration 480
Configuring Rack PDU (Power Strip) Targets 480
Dominion KSX II or SX Configuration 484
Dominion KSX II 484
Dominion SX 489

dcTrack 492
dcTrack Overview 493
Adding the Raritan PX to dcTrack Management 493
RF Code Energy Monitoring Solution 495

Appendix F Additional PX Information 496

MAC Address 496
Locking Outlets and Cords 496
SecureLock™ Outlets and Cords 497
Button-Type Locking Outlets 498
Altitude Correction Factors 499
Data for BTU Calculation 499
Raritan Training Website 500
CLI Command Applicability 500
Show Commands 500
Configuration Commands 502
Other Commands 503
Truncated Data in the Web Interface 504
Reserving IP Addresses in Windows DHCP Servers 504

Index 505

Applicable Models

This user guide is applicable to the **PX2-3nnn**, **PX2-4nnn**, and **PX2-5nnn** series, where n is a number.

Note: For information on PX2-1nnn and PX2-2nnn series, see the "PX-1000/2000 Series" User Guide or online help on the **Raritan website** *(***http://www.raritan.com***).*

Below is a brief comparison between PDU models that are prefixed with *PX2*.

Features	PX2-1nnn	PX2-2nnn	PX2-3nnn (in-line monitors)	PX2-4nnn	PX2-5nnn
Inlet power measurement	Yes	Yes	Yes	Yes	Yes
Outlet power measurement			Yes	Yes	Yes
Outlet switching		Yes			Yes
Load shedding		Yes			Yes
Identical number of inlets and outlets			Yes		
IPv4 support	Yes	Yes	Yes	Yes	Yes
IPv6 support	Yes	Yes	Yes	Yes	Yes
Wired networking	Yes	Yes	Yes	Yes	Yes
Wireless networking	Yes	Yes	Yes	Yes	Yes

Features	PX2-1nnn	PX2-2nnn	PX2-3nnn (in-line monitors)	PX2-4nnn	PX2-5nnn
SNMP v1, v2c and v3	Yes	Yes	Yes	Yes	Yes
Telnet	Yes	Yes	Yes	Yes	Yes
SSH	Yes	Yes	Yes	Yes	Yes
SMTP	Yes	Yes	Yes	Yes	Yes
External authentication, such as LDAP	Yes	Yes	Yes	Yes	Yes
Asset management	Yes	Yes	Yes	Yes	Yes
Local console via USB	Yes	Yes	Yes	Yes	Yes

See ***Product Features*** (on page 1) for more details.

What's New in the PX User Guide

The following sections have changed or information has been added to the PX User Guide based on enhancements and changes to the equipment and/or user documentation.

Checking the Branch Circuit Rating (on page 14)

Installing the USB-to-Serial Driver (Optional) (on page 18)

USB Wireless LAN Adapters (on page 21)

Built-in Wireless LAN Adapters (on page 21)

Supported Wireless LAN Configuration (on page 21)

Cascading the PX via USB (on page 29)

Connecting Detectors/Switches to New DPX-CC2-TR (on page 38)

Contact Closure Sensor LEDs (on page 43)

Floor Water Sensors (on page 43)

Using an X Cable (on page 56)

Connecting a Logitech Webcam (Optional) (on page 58)

Two-Digit Row (on page 67)

Supported Web Browsers (on page 77)

Identifying the Cascaded Devices (on page 95)

Setting Up Default Measurement Units (on page 112)

Setting Up Your Preferred Measurement Units (on page 124)

Enabling and Editing the Security Banner (on page 137)

Setting Up External Authentication (on page 147)

Creating Actions (on page 181)

Setting Thresholds for Multiple Sensors (on page 227)

Sensor Measurement Accuracy (on page 229)

Backup and Restore of PX Device Settings (on page 240)

Snapshot Storage (on page 245)

Managing the Schroff LHX Heat Exchanger (on page 251)

Configuring NTP Server Settings (on page 272)

Using the Command Line Interface (on page 273)

Using the CLI Command (on page 468)

Dominion KSX II or SX Configuration (on page 484)

dcTrack (on page 492)

Raritan Training Website (on page 500)

Reserving IP Addresses in Windows DHCP Servers (on page 504)

Please see the Release Notes for a more detailed explanation of the changes applied to this version of PX.

Chapter 1 Introduction

The Raritan PX is an intelligent power distribution unit (PDU) that allows you to reboot remote servers and other network devices and/or to monitor power in the data center.

The intended use of the Raritan PX is distribution of power to information technology equipment such as computers and communication equipment where such equipment is typically mounted in an equipment rack located in an information technology equipment room.

Raritan offers different types of PDUs -- some are outlet-switching capable, and some are not. With the outlet-switching function, you can recover systems remotely in the event of system failure and/or system lockup, eliminate the need to perform manual intervention or dispatch field personnel, reduce downtime and mean time to repair, and increase productivity.

In This Chapter

Product Models....1
Product Features....1
Package Contents....4

Product Models

The PX comes in several models that are built to stock and can be obtained almost immediately. Raritan also offers custom models that are built to order and can only be obtained on request.

Visit the ***Product Selector page*** (***http://www.raritan.com/resources/px-product-selector/***) on the Raritan website or contact your local reseller for a list of available models.

Product Features

The PX models vary in sizes and features. In general, the PX features include:

- The ability to power on, power off, and reboot the devices connected to each outlet (outlet-switching capable models only)
- The ability to monitor the following at the outlet level:
  - Status (on/off)
  - RMS current (A)
  - RMS voltage (V)
  - Active power (W)

  - Apparent power (VA)
  - Power factor
  - Active energy (Wh)
- The ability to monitor the following at the inlet level:
  - RMS current per line (A)
  - RMS voltage per line pair (V)
  - Active power (W)
  - Apparent power (VA)
  - Power factor
  - Active energy (Wh)
  - Unbalanced load percentage
- The ability to monitor the following at the circuit breaker level:
  - Status (closed/open)
  - Current drawn (A)
  - Current remaining (A)
- The ability to monitor environmental factors such as external temperature and humidity
- User-specified location attributes for environmental sensors
- An audible alarm (beeper) and a visual alarm (blinking LED) to indicate current overload
- The ability to reset the PDU or perform the firmware upgrade without interrupting the operation of connected equipment
- Configurable alarm thresholds and hysteresis
- Configurable assertion timeout for thresholds
- The ability to remotely track the locations of IT devices on the rack through connected asset sensors
- The ability to turn off "non-critical" outlets and keep "critical" outlets turned on when the connected UPS enters the battery-powered mode (outlet-switching capable models only)
- Support for SNMP v1, v2, and v3
- The ability to send traps and informs using the SNMP protocol
- The ability to retrieve outlet specific data using SNMP, including outlet state, current, voltage, and power
- The ability to store a data log of all sensor measurements and retrieve it via SNMP

Note: Raritan's Power IQ or other external systems can retrieve the stored data (samples) from the PX.

- The ability to configure and set values through SNMP, including power threshold levels
- The ability to save one PX device's configuration settings and then deploy those settings to other PX devices
- The ability to back up and restore a PX device's configuration
- Software flippable LED display (Zero U models)
- Support for SSH and Telnet services
- For SSH, both password and public key authentications are supported
- Support for both of IPv4 and IPv6 networking
- Support for Modbus/TCP protocol
- Support for Baytech BSNMP
- Zero configuration service advertisement support
- Wireless connection via a Raritan-provided wireless USB LAN adapter
- The ability to share one Ethernet connection by cascading multiple PX devices via the USB interface
- The ability to visually monitor the data center environment through a connected Logitech® webcam
- Support for webcam images sent via email to designated recipients
- Support of Cinterion® MC52i GSM modems, which allow you to send customized SMS messages to designated recipients for specific events
- The ability to monitor a connected Schroff® LHX-20 or LHX-40 heat exchanger
- Support for Cisco EnergyWise
- Support for RF Code energy monitoring system
- Local overcurrent protection (OCP) via branch circuit breakers or fuses on products rated over 20A to protect connected equipment against overload and short circuits
- The ability to diagnose the network, such as pinging a host or listing TCP connections
- The ability to monitor sever accessibility
- Full disaster recovery option in case of a catastrophic failure during a firmware upgrade
- The ability to display temperatures in Celsius or Fahrenheit, height in meters or feet, and pressure in Pascal or psi according to user credentials
- A combination of outlet types (for example, C13 and C19 outlets) in select models
- A combination of outlet voltages (120 and 208 volts) in select models

- Support for high current devices (such as Blade Servers) in select models
- Support for Gigabit Ethernet (1000Mbit/s) in select models

Package Contents

The following sub-topics describe the equipment and other material included in the product package.

Zero U Products

- The PX device
- Screws, brackets and/or buttons for Zero U
- A null-modem cable with DB9 connectors on both ends (Raritan number: 254-01-0006-00) (optional)
- Cable retention clips for the inlet (for some models only)
- Cable retention clips for outlets (for some models only)

1U Products

- The PX device
- 1U bracket pack and screws
- A null-modem cable with DB9 connectors on both ends (Raritan number: 254-01-0006-00) (optional)
- Cable retention clips for the inlet (for some models only)

2U Products

- The PX device
- 2U bracket pack and screws
- A null-modem cable with DB9 connectors on both ends (Raritan number: 254-01-0006-00) (optional)
- Cable retention clips for the inlet (for some models only)

Chapter 2 Rack-Mounting the PDU

This chapter describes how to rackmount a PX device. Only the most common rackmount method is displayed. Follow the procedure suitable for your model.

In This Chapter

Rackmount Safety Guidelines 5
Circuit Breaker Orientation Limitation.....5
Mounting Zero U Models Using L-Brackets.....6
Mounting Zero U Models Using Button Mount 7
Mounting Zero U Models Using Claw-Foot Brackets 9
Mounting Zero U Models Using Two Rear Buttons.....10
Mounting 1U or 2U Models.....11

Rackmount Safety Guidelines

In Raritan products which require rack mounting, follow these precautions:

- Operation temperature in a closed rack environment may be greater than room temperature. Do not exceed the rated maximum ambient temperature of the Power Distribution Units. See ***Specifications*** (on page 460) in the User Guide.
- Ensure sufficient airflow through the rack environment.
- Mount equipment in the rack carefully to avoid uneven mechanical loading.
- Connect equipment to the supply circuit carefully to avoid overloading circuits.
- Ground all equipment properly, especially supply connections, to the branch circuit.

Circuit Breaker Orientation Limitation

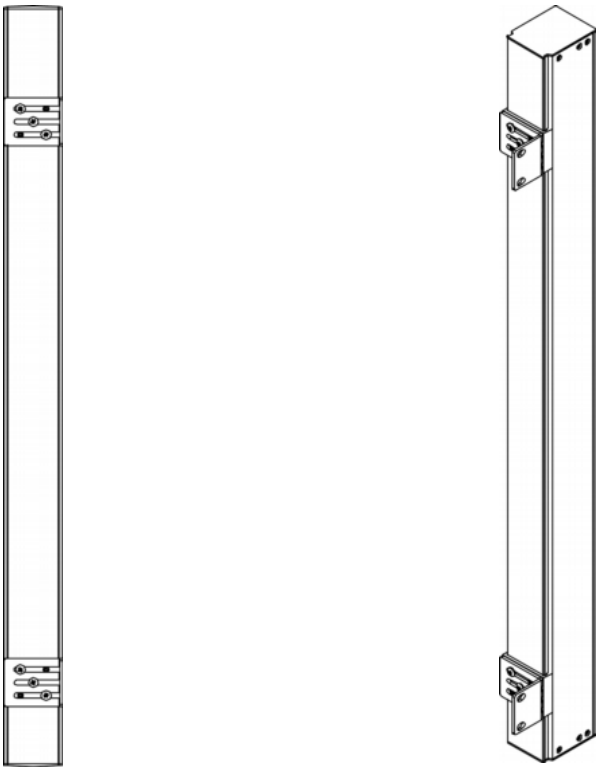
Usually a PDU can be mounted in any orientation. However, when mounting a PDU with circuit breakers, you must obey these rules:

- Circuit breakers CANNOT face down. For example, do not horizontally mount a Zero U PDU with circuit breakers on ceiling.
- If a rack is subject to shock in environments such as boats or airplanes, the PDU CANNOT be mounted upside down. If installed upside down, shock stress reduces the trip point by 10%.

Note: If normally the line cord is down, upside down means the line cord is up.

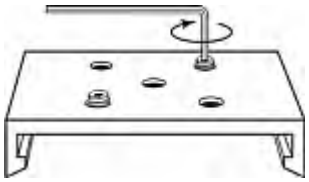
Mounting Zero U Models Using L-Brackets

If your PDU has circuit breakers implemented, read ***Circuit Breaker Orientation Limitation*** (on page 5) before mounting it.

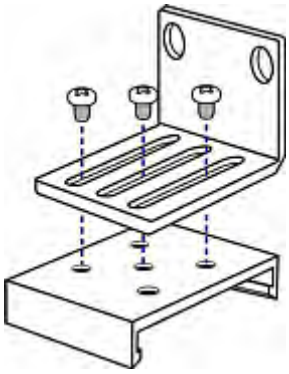


To mount Zero U models using L-brackets:

1. Align the baseplates on the rear of the PX device.
2. Secure the baseplates in place. Use the included L-shaped hex key to loosen the hex socket screws until the baseplate is "slightly" fastened.



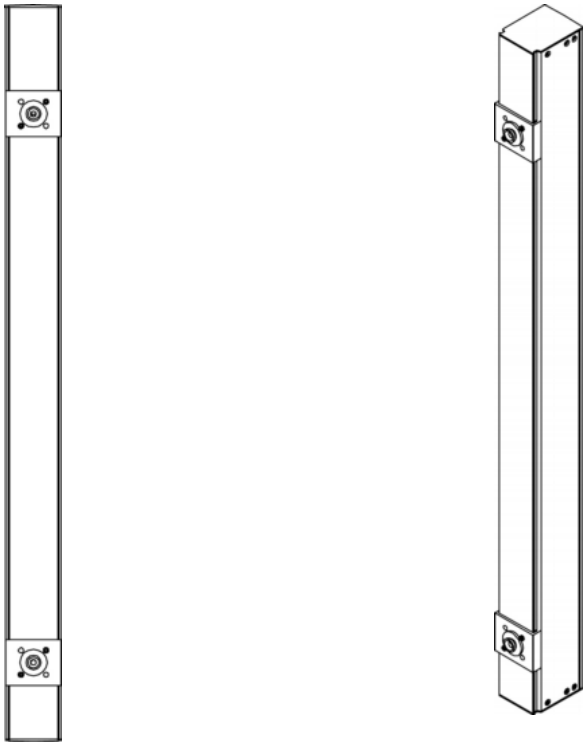
3. Align the L-brackets with the baseplates so that the five screw-holes on the baseplates line up through the L-bracket's slots. The rackmount side of brackets should face either the left or right side of the PX device.
4. Fasten the brackets in place with at least three screws (one through each slot). Use additional screws as desired.



5. Using rack screws, fasten the PX device to the rack through the L-brackets.

Mounting Zero U Models Using Button Mount

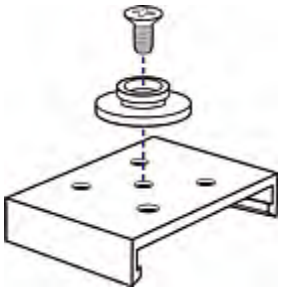
If your PDU has circuit breakers implemented, read ***Circuit Breaker Orientation Limitation*** (on page 5) before mounting it.



To mount Zero-U models using button mount:

1. Align the baseplates on the rear of the PX device. Leave at least 24 inches between the baseplates for stability.

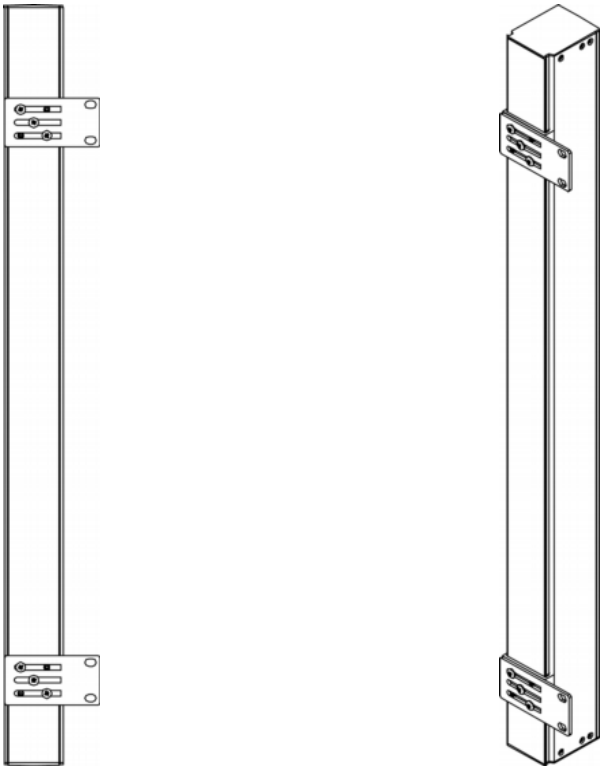
2. Make the baseplates grasp the PX device lightly. Use the included L-shaped hex key to loosen the hex socket screws until the baseplate is "slightly" fastened.
3. Screw each mounting button in the center of each baseplate. The recommended torque for the button is 1.96 N·m (20 kgf·cm).



4. Align the large mounting buttons with the mounting holes in the cabinet, fixing one in place and adjusting the other.
5. Loosen the hex socket screws until the mounting buttons are secured in their position.
6. Ensure that both buttons can engage their mounting holes simultaneously.
7. Press the PX device forward, pushing the mounting buttons through the mounting holes, then letting the device drop about 5/8". This secures the PX device in place and completes the installation.

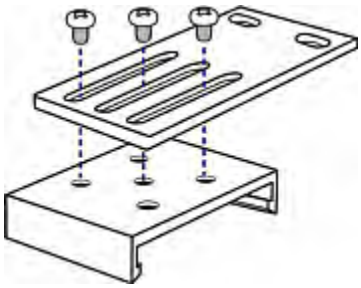
Mounting Zero U Models Using Claw-Foot Brackets

If your PDU has circuit breakers implemented, read ***Circuit Breaker Orientation Limitation*** (on page 5) before mounting it.



To mount Zero U models using claw-foot brackets:

1. Align the baseplates on the rear of the PX device.
2. Secure the baseplates in place. Use the included L-shaped hex key to loosen the hex socket screws until the baseplate is "slightly" fastened.
3. Align the claw-foot brackets with the baseplates so that the five screw-holes on the baseplates line up through the bracket's slots. The rackmount side of brackets should face either the left or right side of the PX device.
4. Fasten the brackets in place with at least three screws (one through each slot). Use additional screws as desired.



5. Using rack screws, fasten the PX device to the rack through the claw-foot brackets.

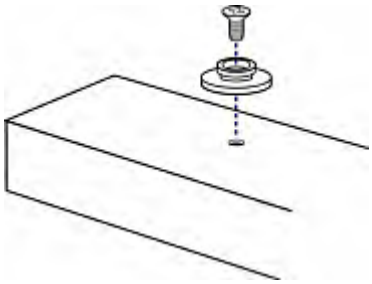
Mounting Zero U Models Using Two Rear Buttons

The following describes how to mount a PDU using two buttons only. If your PDU has circuit breakers implemented, read ***Circuit Breaker Orientation Limitation*** (on page 5) before mounting it.

To mount Zero U models using two buttons:

1. Turn to the rear of the PDU.
2. Locate two screw holes on the rear panel: one near the bottom and the other near the top (the side of cable gland).

3. Screw a button in the screw hole near the bottom. The recommended torque for the button is 1.96 N·m (20 kgf·cm).



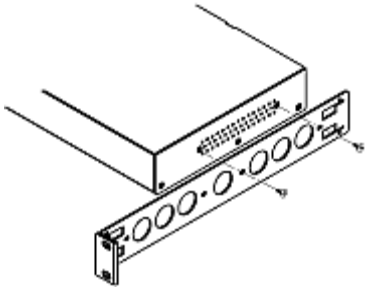
4. Screw a button in the screw hole near the top. The recommended torque for the button is 1.96 N·m (20 kgf·cm).
5. Ensure that the two buttons can engage their mounting holes in the rack or cabinet simultaneously.
6. Press the PX device forward, pushing the mounting buttons through the mounting holes, then letting the device drop slightly. This secures the PX device in place and completes the installation.

Mounting 1U or 2U Models

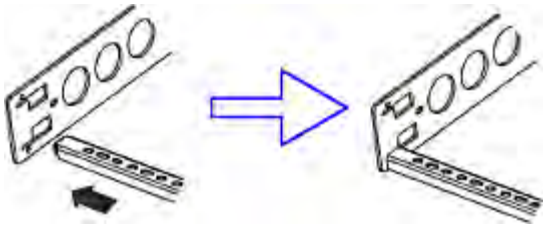
Using the appropriate brackets and tools, fasten the 1U or 2U PX device to the rack or cabinet. If your PDU has circuit breakers implemented, read ***Circuit Breaker Orientation Limitation*** (on page 5) before mounting it.

To mount the PX device:

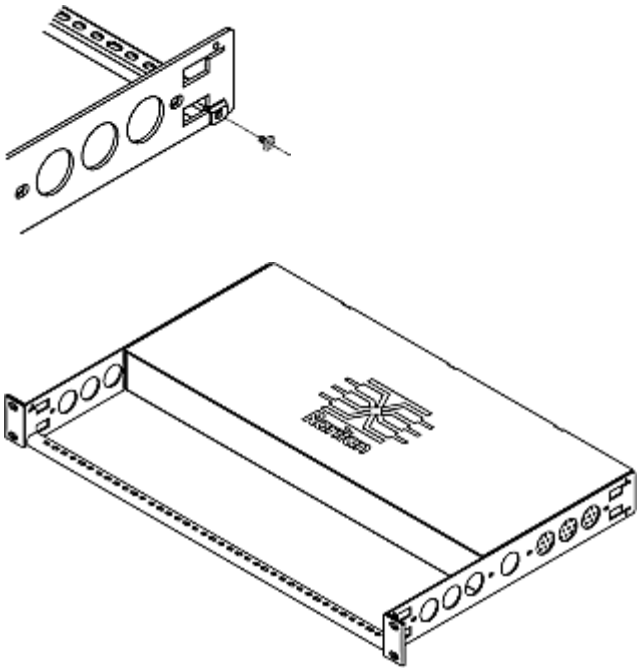
1. Attach a rackmount bracket to each side of the PX with the provided screws.



2. Insert the cable-support bar into rackmount brackets.



3. Secure with the provided end cap screws.



4. Mount the PX device on the rack by securing the rackmount brackets' ears to the rack's front rails with your own screws, bolts, cage nuts, or the like.

Chapter 3 Installation and Configuration

This chapter explains how to install a PX device and configure it for network connectivity.

In This Chapter

Before You Begin 13
Installing Cable Retention Clips on the Inlet (Optional).....14
Connecting the PDU to a Power Source 15
Configuring the PX 16
Cascading the PX via USB.....29
Installing Cable Retention Clips on Outlets (Optional) 31

Before You Begin

Before beginning the installation, perform the following activities:

- Unpack the product and components
- Prepare the installation site
- Fill out the equipment setup worksheet
- Check the branch circuit rating

Unpacking the Product and Components

1. Remove the PX device and other equipment from the box in which they were shipped. See ***Package Contents*** (on page 4) for a complete list of the contents of the box.
2. Compare the serial number of the equipment with the number on the packing slip located on the outside of the box and make sure they match.
3. Inspect the equipment carefully. If any of the equipment is damaged or missing, contact Raritan's Technical Support Department for assistance.
4. Verify that all circuit breakers on the PX device are set to ON. If not, turn them ON.

   For a PDU with fuses, ensure that all fuses are inserted and seated properly. If there are any fuse covers, ensure that they are closed.

   Note: Not all PX devices have overcurrent protection mechanisms.

Preparing the Installation Site

1. Make sure the installation area is clean and free of extreme temperatures and humidity.

Note: If necessary, contact Raritan Technical Support for the maximum operating temperature for your model. See **Maximum Ambient Operating Temperature** *(on page 460).*

2. Allow sufficient space around the PX device for cabling and outlet connections.
3. Review the ***Safety Instructions*** (on page iii) listed in the beginning of this user guide.

Checking the Branch Circuit Rating

This section describes the rating of the branch circuit supplying power to the PDU:

- The rating of the branch circuit shall be in accordance with national and local electrical codes.
- For North American, the rating of the branch circuit may be up to 125% greater than the rating of the PDU, unless prohibited by national or local electrical codes.
- In North America, external overcurrent protectors shall be certified by UL/CSA (or equivalent certification). In other regions or countries, make sure they comply with national and local electrical codes.

Filling Out the Equipment Setup Worksheet

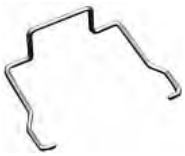
An Equipment Setup Worksheet is provided in this guide. See ***Equipment Setup Worksheet*** (on page 463). Use this worksheet to record the model, serial number, and use of each IT device connected to the PDU.

As you add and remove devices, keep the worksheet up-to-date.

Installing Cable Retention Clips on the Inlet (Optional)

If your PX device is designed to use a cable retention clip, install the clip before connecting a power cord. A cable retention clip prevents the connected power cord from coming loose or falling off.

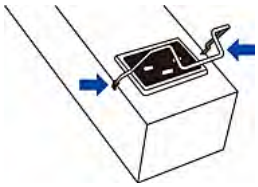
The use of cable retention clips is highly recommended for regions with high seismic activities, and environments where shocks and vibrations are expected.



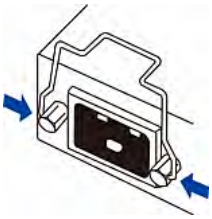
To install and use a cable retention clip on the inlet:

1. Locate two tiny holes adjacent to the inlet.
2. Install the cable retention clip by inserting two ends of the clip into the tiny holes.

Zero U models

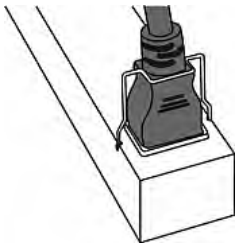


1U/2U models

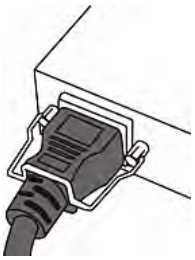


3. Connect the power cord to the inlet, and press the clip toward the power cord until it holds the cord firmly.

Zero U models



1U/2U models



Connecting the PDU to a Power Source

1. Verify that all circuit breakers on the PX device are set to ON. If not, turn them ON.

   For a PDU with fuses, ensure that all fuses are inserted and seated properly. If there are any fuse covers, ensure that they are closed.

   Note: Not all PX devices have overcurrent protection mechanisms.

2. Connect each PX device to an appropriately rated branch circuit. See the label or nameplate affixed to your PX device for appropriate input ratings or range of ratings.

   Note: When a PX device powers up, it proceeds with the power-on self test and software loading for a few moments. At this time, the outlet LEDs cycle through different colors.

   Note: Outlet LEDs are only available on an outlet-switching capable PDU.

3. When the software has completed loading, the outlet LEDs show a steady color and the LED display illuminates.

Configuring the PX

There are two ways to initially configure a PX device:

- Connect the PX device to a computer to configure it, using a serial or USB connection between the PX and the computer.

  The computer must have a communications program such as HyperTerminal or PuTTY.

  For a serial connection, you need a null-modem cable with DB9 connectors on both ends (Raritan part number: 254-01-0006-00).

- Connect the PX device to a TCP/IP network that supports DHCP, and use the IP address and web browser to remotely configure the PX.

  The DHCP-assigned IP address can be retrieved through the PX device's MAC address. You can contact your LAN administrator for assistance. See ***MAC Address*** (on page 496).

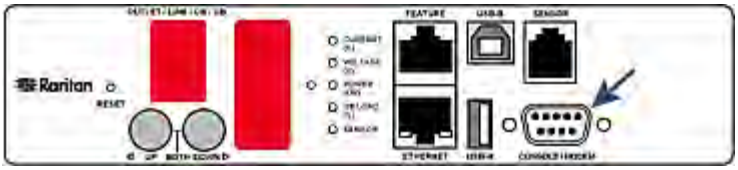
  A Category 5e/6 UTP cable is required for a wired network connection.

Connecting the PX to a Computer

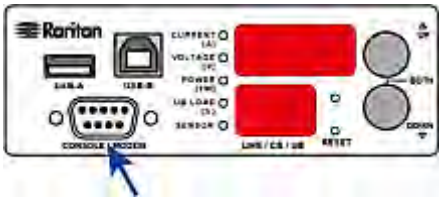
To configure the PX using a computer, it must be connected to the computer with an RS-232 serial interface.

These diagrams show the serial port location on different types of PDUs.

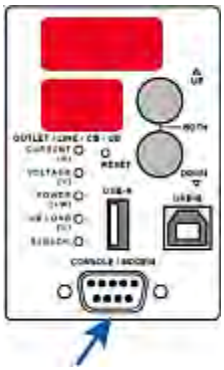
Zero U models:



1U models:



2U models:



If your computer does not have a serial port, use a regular USB cable to connect the PX to the computer for initial configuration. The PX device can emulate a serial port after the USB-to-serial driver is properly installed in the Windows® operating system.

Note: Not all serial-to-USB converters work properly with the PX device so this section does not introduce the use of such converters.

Connect the PX to a computer for initial configuration by following either of the procedures below.

▶ To make a serial connection:

1. Connect one end of the null-modem cable to the RS-232 port labeled CONSOLE / MODEM on the PX.
2. Connect the other end of the null-modem cable to the serial port (COM) on the computer.

To make a USB connection:

1. The USB-to-serial driver is required in Windows® for a USB connection. If using a computer running Windows®, it is recommended to perform automatic driver installation before connecting the USB cable. See ***Installing the USB-to-Serial Driver (Optional)*** (on page 18) for details.
2. Connect one end of a regular USB cable to the USB-B port on the PX.
3. Connect the other end of the USB cable to the USB-A port on the computer.

Note: If you plan to use the serial connection to log in to the command line interface, leave the cable connected after the configuration is complete.

Installing the USB-to-Serial Driver (Optional)

The PX can emulate a serial port over a USB connection. A USB-to-serial driver named "Dominion Serial Console" is required for Microsoft® Windows® operating systems, including Windows® XP, Vista, 7 and 8. Download the *dominion-serial* driver file, which contains *dominion-serial.inf*, *dominion-serial.cat* and *dominion-serial-setup-2.0.exe* files, from the PX 2.4.0 section on the Raritan website's ***Firmware and Documentation section*** (***http://www.raritan.com/support/firmware-and-documentation/***).

There are two ways to install this driver in Windows®: automatic and manual installation. Automatic driver installation is highly recommended. You should perform manual driver installation only if the automatic installation fails.

Automatic driver installation in Windows®:

1. Make sure the PX device is NOT connected to the computer via a USB cable.
2. Run dominion-serial-setup-2.0.exe. A Dominion Serial Console Driver Setup Wizard appears.

   Note: If any Windows security warning appears, accept it to continue the installation.
3. Click Install to install the driver.
4. Click Finish when the installation is complete.

5. Connect the PX device's USB cable back to the computer. The driver is automatically installed.

Manual driver installation in Windows®:

1. Make sure the PX device has been connected to the computer via a USB cable.
2. The computer detects the new device and the "Found New Hardware Wizard" dialog appears. If this dialog does not appear, choose Control Panel > System > Hardware > Device Manager, right-click the *xxx Serial Console* (where xxx represents the product name), and choose Update Driver.
3. Select the option of driver installation from a specific location, and then specify the location where both the *dominion-serial.inf* and *dominion-serial.cat* are stored.

   Note: If any Windows security warning appears, accept it to continue the installation.

4. Wait until the installation is complete.

Note: If the PX enters the disaster recovery mode when the dominion serial driver is not installed yet, it may be shown as a 'GPS camera' in the Device Manager on the computer connected to it.

In Linux:

No additional drivers are required, but you must provide the name of the tty device, which can be found in the output of the "dmesg" after connecting the PX to the computer. Usually the tty device is "/dev/ttyACM#" or "/dev/ttyUSB#," where # is an integer number.

For example, if you are using the kermit terminal program, and the tty device is "/dev/ttyACM0," perform the following commands:

> set line /dev/ttyACM0

> connect

Connecting the PX to Your Network

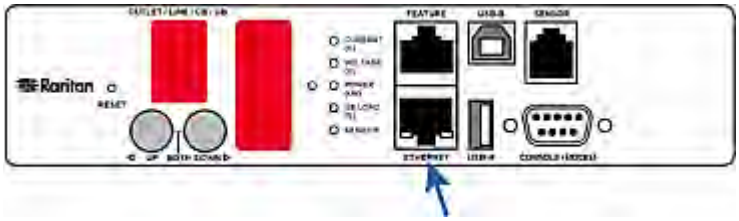
To use the web interface to administer the PX, you must connect the PX to your local area network (LAN). The PX can be connected to a wired or wireless network.

Note: If your PDU is not implemented with the wireless networking feature or if it will be used as a master device in the USB cascading configuration, make a wired connection.

To make a wired connection:

1. Connect a standard Category 5e/6 UTP cable to the ETHERNET port on the PX.
2. Connect the other end of the cable to your LAN.

   See this diagram for the ETHERNET port location on Zero U models.



For 1U/2U models, the ETHERNET port is usually located on the back except for a few models. This diagram shows the port on the back.

Warning: Accidentally plugging an RS-232 RJ-45 connector into the ETHERNET port can cause permanent damages to the Ethernet hardware.

To make a wireless connection:

Do one of the following:

- Plug a supported USB wireless LAN adapter into the USB-A port on your PX.
- Connect a USB docking station to the USB-A port on the PX and plug the supported USB wireless LAN adapter into the appropriate USB port on the docking station.

See ***USB Wireless LAN Adapters*** (on page 21) for a list of supported wireless LAN adapters.

USB Wireless LAN Adapters

The following table lists USB wireless LAN adapters that the PX supports.

Wi-Fi LAN adapter	Supported 802.11 protocols
Proxim Orinoco 8494	A/B/G
Zyxel NWD271N	B/G
Edimax EW-7722UnD	A/B/G/N

Note: To use the Edimax EW-7722UnD wireless LAN adapter to connect to an 802.11n *wireless network, the handshake timeout setting must be changed to 500 or greater, or the wireless connection will fail.*

Built-in Wireless LAN Adapters

If the Raritan product you purchased has been implemented with the following 802.11 wireless LAN adapter when shipping out of the factory, no USB wireless LAN adapters are required to make a wireless connection.

Wi-Fi LAN adapter	Supported 802.11 protocols
HD-Wireless	B/G

Supported Wireless LAN Configuration

If a wireless connection is preferred, ensure that the wireless LAN configuration of your PX matches the access point. The following is the wireless LAN configuration that the PX supports.

- Network type: 802.11 A/B/G/N
- Protocol: WPA2 (RSN)
- Key management: WPA-PSK, or WPA-EAP with PEAP and MSCHAPv2 authentication
- Encryption: CCMP (AES)

Important: Raritan only supports specific wireless LAN adapters. Supported 802.11 network protocols vary according to the wireless LAN adapter being used with the PX. See *USB Wireless LAN Adapters* **(on page 21).**

Initial Network Configuration

After the PX device is connected to your network, you must provide it with an IP address and some additional networking information.

This section describes the initial configuration via a serial or USB connection.

Note: To configure the PX via the LAN, see **Using the Web Interface** *(on page 77) for using the web interface.*

To configure the PX device:

1. Go to the computer that you connected to the PX and open a communications program such as HyperTerminal or PuTTY.
2. Select the appropriate COM port, and make sure the port settings are configured as follows:
   - Bits per second = 115200 (115.2Kbps)
   - Data bits = 8
   - Stop bits = 1
   - Parity = None
   - Flow control = None

   Tip: For a USB connection, you can find out which COM port is assigned to the PX by choosing Control Panel > System > Hardware > Device Manager, and locating the "XXX Serial Console" under the Ports group, where XXX represents this product's name.
3. Press Enter.
4. The PX prompts you to log in. Note that both of user name and password are case sensitive.
   a. At the Username prompt, type `admin` and press Enter.
   b. At the Password prompt, type `raritan` and press Enter.
5. You are prompted to change the password if this is the first time you log in to the PX. Follow the onscreen instructions to type your new password.
6. The # prompt appears when you log in successfully.
7. Type `config` and press Enter.
8. To configure network settings, type appropriate commands, and press Enter. All commands are case sensitive.
   a. To set the networking mode, type this command:

   ```
   network mode <mode>
   ```

where <mode> is either *wired* for wired connection (default) or *wireless* for wireless connection.

b. For the wired network mode, you may configure the LAN interface settings. In most scenarios, the default setting (auto) works well and should not be changed unless required.

To set	Use this command
LAN interface speed	`network interface LANInterfaceSpeed <option>` where <option> is *auto*, *10Mbps*, or *100Mbps*.
LAN interface duplex mode	`network interface LANInterfaceDuplexMode <mode>` where <mode> is *half*, *full* or *auto*.

Tip: You can combine multiple commands to configure multiple parameters at a time. For example,
`network interface LANInterfaceSpeed <option> LANInterfaceDuplexMode <mode>`

c. For the wireless network mode, you must configure the Service Set Identifier (SSID) parameter.

To set	Use this command
SSID	`network wireless SSID <ssid>` where <ssid> is the SSID string.

If necessary, configure more wireless parameters shown in the following table.

To set	Use this command
BSSID	`network wireless BSSID <bssid>` where <bssid> is the AP MAC address or *none* if not available.

To set	Use this command
Authentication method	`network wireless authMethod <method>` where <method> is *psk* for Pre-Shared Key or *eap* for Extensible Authentication Protocol.
PSK	`network wireless PSK <psk>` where <psk> is the PSK string.
EAP outer authentication	`network wireless eapOuterAuthentication <outer_auth>` where <outer_auth> is *PEAP*.
EAP inner authentication	`network wireless eapInnerAuthentication <inner_auth>` where <inner_auth> is *MSCHAPv2*.
EAP identity	`network wireless eapIdentity <identity>` where <identity> is your user name for EAP authentication.
EAP password	`network wireless eapPassword` When prompted to enter the password for EAP authentication, type the password.
EAP CA certificate	`network wireless eapCACertificate` When prompted to enter the CA certificate, open the certificate with a text editor, copy and paste the content into the communications program.

Note: The content to be copied from the CA certificate does NOT include the first line containing "BEGIN CERTIFICATE" and the final line containing "END CERTIFICATE."

d. To determine which IP protocol is enabled and which IP address returned by the DNS server is used, configure the following parameters.

To set	Use this command
IP protocol	`network ip proto <protocol>` where <protocol> is *v4Only* for enabling IPv4, *v6Only* for enabling IPv6 or *both* for enabling both IPv4 and IPv6 protocols.
IP address returned by the DNS server	`network ip dnsResolverPreference <resolver>` where <resolver> is *preferV4* for IPv4 addresses or *preferV6* for IPv6 addresses.

e. If you enabled the IPv4 protocol in the previous step, configure the IPv4 network parameters.

To set	Use this command
IP configuration method	`network ipv4 ipConfigurationMode <mode>` where <mode> is either *dhcp* for auto configuration (default) or *static* for specifying a static IP address.

- For the IPv4 DHCP configuration, configure this parameter.

To set	Use this command
Preferred host name (optional)	`network ipv4 preferredHostName <name>` where <name> is the preferred host name.

Tip: To override the DHCP-assigned IPv4 DNS servers with those you specify manually, type this command:

`network ipv4 overrideDNS <option>`

where <option> is `enable` or `disable`. See the table below for the IPv4 commands for manually specifying DNS servers.

- For the static IPv4 configuration, configure these parameters.

To set	Use this command
Static IPv4 address	`network ipv4 ipAddress <ip address>` where <ip address> is the IP address you want to assign.
Subnet mask	`network ipv4 subnetMask <netmask>` where <netmask> is the subnet mask.
Gateway	`network ipv4 gateway <ip address>` where <ip address> is the IP address of the gateway.
Primary DNS server	`network ipv4 primaryDNSServer <ip address>` where <ip address> is the IP address of the primary DNS server.
Secondary DNS server (optional)	`network ipv4 secondaryDNSServer <ip address>` where <ip address> is the IP address of the secondary DNS server.

f. If you enabled IPv6 in the earlier step, configure the IPv6 network parameters.

To set	Use this command
IP configuration method	`network ipv6 ipConfigurationMode <mode>` where <mode> is either *automatic* for auto configuration (default) or *static* for specifying a static IP address.

- For the IPv6 DHCP (automatic) configuration, configure this parameter.

To set	Use this command
Preferred host name (optional)	`network ipv6 preferredHostName <name>` where <name> is the preferred host name.

Tip: To override the DHCP-assigned IPv6 DNS servers with those you specify manually, type this command:

`network ipv6 overrideDNS <option>`

where <option> is `enable` or `disable`. See the table below for the IPv6 commands for manually specifying DNS servers.

- For the static IPv6 configuration, you should configure the following parameters. Note that the IP address must follow the IPv6 format.

To set	Use this command
Static IPv6 address	`network ipv6 ipAddress <ip address>` where <ip address> is the IP address you want to assign.
Gateway	`network ipv6 gateway <ip address>` where <ip address> is the IP address of the gateway.
Primary DNS server	`network ipv6 primaryDNSServer <ip address>` where <ip address> is the IP address of the primary DNS server.
Secondary DNS server (optional)	`network ipv6 secondaryDNSServer <ip address>` where <ip address> is the IP address of the secondary DNS server.

9. To quit the configuration mode with or without saving the changes, type either command, and press Enter.

Command	Description
`apply`	Save all configuration changes and quit the configuration mode.
`cancel`	Abort all configuration changes and quit the configuration mode.

The # prompt appears, indicating that you have quit the configuration mode.

10. To verify whether all settings are correct, type the following commands one by one. Current network settings are displayed.

Command	Description
`show network`	Show network parameters.
`show network ip all`	Show all IP configuration parameters.
`show network wireless details`	Show all wireless parameters. (Perform this command only when you enable the wireless mode.)

Tip: You can also type "`show network wireless`" to display a shortened version of wireless settings.

11. If all are correct, type `exit` to log out of the PX. If any are incorrect, repeat Steps 7 to 10 to change any network settings.

The IP address configured may take seconds to take effect.

Cascading the PX via USB

Up to four (4) devices are supported as part of a daisy chain. This daisy chain feature permits multiple PX devices to be cascaded using USB cables, sharing the Ethernet connectivity accordingly. Different models can be cascaded as long as they are running the supported firmware.

The first device in the chain is the master device and all subsequent devices connected to it are slave devices. All devices in the chain are accessible over an IP network, with the master PX acting as a network bridge. Therefore, you can access individual devices via the Web, SNMP, SSH or Telnet interface no matter they are master or slave devices.

The USB-cascading configuration only supports *wired* networking so you must make sure:

- The master device has "wired" Ethernet connectivity.
- None of the slave devices has wired Ethernet connectivity. Even though you connect any slave device to the LAN through a network cable, its wired Ethernet interface is automatically disabled.
- None of the devices in the chain has wireless connectivity.

Important: Only PX devices whose model names begin with PX2 support the USB-cascading function.

For more information on the USB-cascading configuration, see the *USB-Cascading Solution User Guide*, which is available on the ***PX2 web page*** (***http://www.raritan.com/support/dominion-px2/***) of the Raritan website.

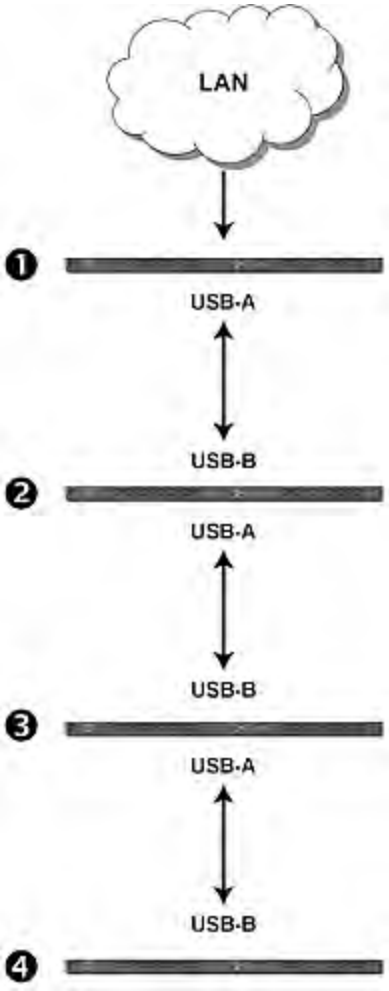
To cascade the PX devices via USB:

1. Verify that the PX devices to be cascaded are running the following firmware version by choosing Maintenance > Device Information in the web interface or using CLI's `show pdu` command. If not, upgrade these devices. See ***Updating the PX Firmware*** (on page 258).
   - Raritan PX: version 2.3.1 or later
2. Select one of the four devices as the master device and connect this device to the LAN via a standard Category 5e/6 UTP cable.
3. Connect the USB-A port of the master device to the USB-B port of an additional PX via a USB cable. This additional device is Slave 1.

   Do not connect Slave 1 to the LAN.
4. Connect Slave 1's USB-A port to the USB-B port of an additional PX via a USB cable. The second additional device is Slave 2.

   Do not connect Slave 2 to the LAN.
5. Connect Slave 2's USB-A port to the USB-B port of another PX via a USB cable. The final additional device is Slave 3.

Do not connect Slave 3 to the LAN.



Number	Device role
❶	Master device
❷	Slave 1
❸	Slave 2
❹	Slave 3

Note: On a master device, the networking mode shows "Wired." On a slave device, the networking mode shows "Wired(USB)." See **Identifying the Cascaded Devices** *(on page 95).*

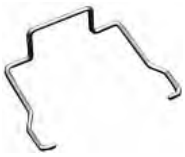
Tip: The USB-cascading configuration can be a mixture of diverse Raritan products that support the USB-cascading feature, such as Raritan PX and EMX. Note that it requires the EMX firmware version 2.2 or later to support this USB-cascading function. The limit of up to four Raritan devices in one USB-cascading configuration remains unchanged.

Installing Cable Retention Clips on Outlets (Optional)

If your PX device is designed to use a cable retention clip, install the clip before connecting a power cord. A cable retention clip prevents the connected power cord from coming loose or falling off.

The use of cable retention clips is highly recommended for regions with high seismic activities, and environments where shocks and vibrations are expected.

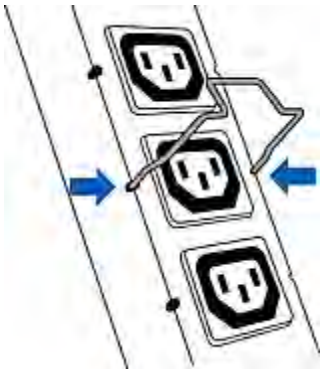
These optional clips come in various sizes to accommodate diverse power cords used on IT equipment, which are connected to C13 or C19 outlets. You can request a cable retention kit containing different sizes of clips from you reseller. Make sure you use a clip that fits the power cord snugly to facilitate the installation or removal operation (for servicing).



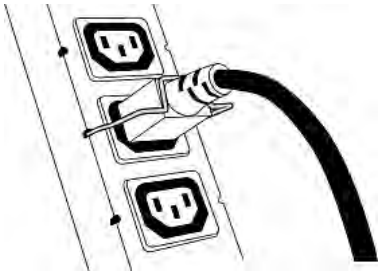
Note: Some NEMA sockets on PSE-certified PDUs for Japan have integral locking capability and do not need cable retention clips.

To install and use a cable retention clip on the outlet:

1. Locate two tiny holes adjacent to the outlet.
2. Install the cable retention clip by inserting two ends of the clip into the tiny holes.



3. Plug the power cord into the outlet, and press the clip toward the power cord until it holds the cord firmly. The clip's central area holding the plug should face downwards toward the ground, like an inverted "U". This allows gravity to keep the clip in place.



4. Repeat the same steps to install clips and power cords on the other outlets.

Tip: Raritan also provides other mechanisms to securely hold the power cords in place. See **Locking Outlets and Cords** *(on page 496).*

Chapter 4 Connecting External Equipment

More features are available in addition to remotely monitoring and managing this PX if you connect Raritan's or third-party external equipment to your PX.

In This Chapter

Connecting Environmental Sensors (Optional) 33
Connecting the Asset Management Sensor (Optional).....47
Connecting a Logitech Webcam (Optional).....58
Connecting a GSM Modem (Optional) 59
Connecting a Schroff LHX Heat Exchanger (Optional) 59
Connecting an RF Code PDU Sensor Tag (Optional).....60

Connecting Environmental Sensors (Optional)

To enable the detection of environmental factors around the PX, connect one or more Raritan environmental sensors to the PX device.

The maximum distance for all sensor cabling plugged into the product's sensor port should not exceed 30 meters/100 feet. Contact Raritan Technical Support if you have questions.

You can connect up to 16 environmental sensors to a PX device by using a Raritan sensor hub.

Note that a Raritan environmental sensor usually contains more than one sensor. For example, a DPX-T2H2 counts as 4 sensors, and a DPX-T3H1 counts as 4 sensors.

Warning: For proper operation, wait for 15~30 seconds between each connection operation or each disconnection operation of environmental sensors.

To directly connect one or multiple environmental sensors:

- Plug the connector of the environmental sensor into the SENSOR port on your PX device.

Note: Depending on the model you purchased, the total number of SENSOR ports varies.

To connect environmental sensors via an optional PX sensor hub:

1. Connect a Raritan sensor hub to the PX device.
   a. Plug one end of the Raritan-provided phone cable (4-wire, 6-pin, RJ-12) into the IN port (Port 1) of the hub.

b. Plug the other end into the SENSOR port on the PX device.

2. Connect Raritan environmental sensors to any of the four OUT ports on the hub.

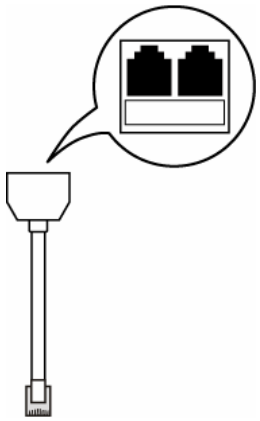
   Raritan sensor hubs CANNOT be cascaded so at most a sensor hub can be connected to each SENSOR port on the PX device. This diagram illustrates a configuration with a sensor hub connected.

❶	The PX device
❷	Raritan-provided phone cable
❸	Raritan PX sensor hub
❹	Raritan environmental sensors

To connect environmental sensors via a Raritan Y cable:

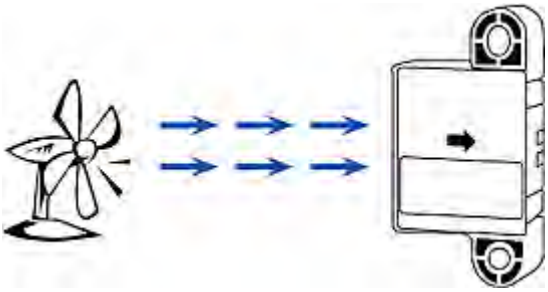
1. Plug the connector of a Y cable into the SENSOR port on your PX device.

2. A Y cable has two sensor ports. Plug Raritan environmental sensors into the Y cable's sensor ports.



3. Repeat the above steps if there are additional SENSOR ports on your PX model.

If there are any Raritan air flow sensors attached, make sure that sensor faces the source of the wind (such as a fan) in the appropriate orientation as indicated by the arrow on that sensor.



Contact Closure Sensors

Raritan's contact closure sensor (DPX-CC2-TR) can detect the open-and-closed status of the connected detectors/switches.

This feature requires the integration of at least a discrete (on/off) detector/switch to work properly. The types of discrete detectors/switches that can be plugged into DPX-CC2-TR include those for:

- Door open/closed detection
- Door lock detection
- Floor water detection
- Smoke detection
- Vibration detection

Raritan does NOT produce most of the above detectors/switches except floor water sensors. When using third-party probes, you must test them with Raritan's DPX-CC2-TR to ensure they work properly.

Important: Integration and testing for third-party detectors/switches is the

sole responsibility of the customer. Raritan cannot assume any liability as a result of improper termination or failure (incidental or consequential) of third-party detectors/switches that customers provide and install. Failure to follow installation and configuration instructions can result in false alarms or no alarms. Raritan makes no statement or claim that all third-party detectors/switches will work with DPX-CC2-TR.

Raritan has changed the design of contact closure sensors and made new contact closure sensors available for sale since the 4th quarter of 2012. Both old and new contact closure sensors function in the same manner, and the latest PX firmware supports the use of either one. See ***Old and New Contact Closure Sensors*** (on page 36) for details.

Old and New Contact Closure Sensors

Raritan further improved the design of contact closure sensors and released a second version in the 4th quarter of 2012. Old and new contact closure sensors are functionally identical. The major difference between them is the mechanical design as described below.

- The old sensor uses tiny buttons to secure or loosen wires of the connected detectors/switches while the new sensor uses tiny screws.
- The new sensor has a separate terminal module so that it is more convenient to connect or disconnect all connected detectors/switches from the contact closure sensor.

Both old and new contact closure sensors share the same part number: *DPX-CC2-TR*.

New type of DPX-CC2-TR is supported as of release 2.4 so make sure you are running the firmware version 2.4 or later when using new DPX-CC2-TR. The latest PX firmware continuously supports old type of DPX-CC2-TR.

- For instructions on *old* contact closure sensors, see ***Connecting Detectors/Switches to DPX-CC2-TR*** (on page 37).
- For instructions on *new* contact closure sensors, see ***Connecting Detectors/Switches to New DPX-CC2-TR*** (on page 38).

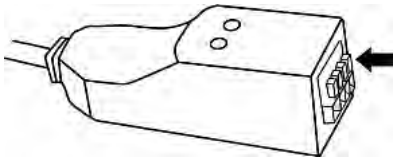
Connecting Detectors/Switches to DPX-CC2-TR

A DPX-CC2-TR unit provides two channels for connecting two discrete (on/off) detectors/switches. There are four spring-loaded termination points on the body of DPX-CC2-TR: the two to the right are associated with one channel (as indicated by the LED number), and the two to the left are associated with the other. You must plug discrete detectors/switches into these termination points.

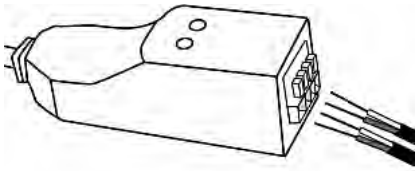
To connect third-party or Raritan's discrete detectors/switches:

1. Strip the insulation around 12mm from the end of each wire of discrete detectors/switches.
2. Press and hold down the tiny rectangular buttons above the termination points on the body of DPX-CC2-TR.

Note: Each button controls the spring of each corresponding termination point.



3. Fully insert each wire of both detectors/switches into each termination point.
   - Plug both wires of a detector/switch into the two termination points to the left.
   - Plug both wires of the other detector/switch into the two termination points to the right.



4. Release the tiny rectangular buttons after inserting the wires properly.
5. Verify that these wires are firmly fastened.
6. If the detector/switch plugged into the contact closure sensor is Raritan's floor water sensor, verify that the total cable length from the port of the PX to the water detector does not exceed 30 meters/100 feet.

Connecting Detectors/Switches to New DPX-CC2-TR

Like the old DPX-CC2-TR, a new DPX-CC2-TR unit also provides two channels for connecting two discrete (on/off) detectors/switches. Four termination points are also available on this new sensor: the two to the right are associated with one channel (as indicated by the LED number), and the two to the left are associated with the other.

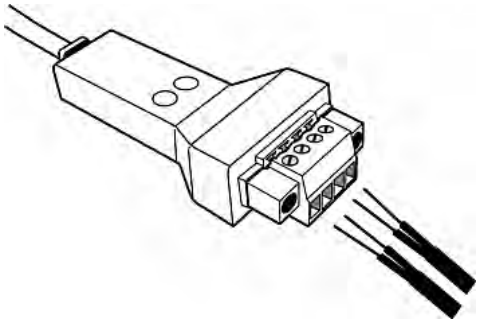
If the detector/switch plugged into the contact closure sensor is Raritan's floor water sensor, verify that the total cable length from the port of the PX to the water detector does not exceed 30 meters/100 feet.

The new contact closure sensor comprises two parts: sensor module and terminal module. The terminal module is removable. With this design, There are two ways to plug discrete detectors/switches:

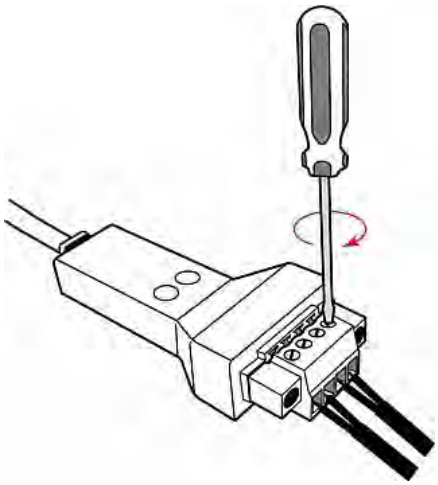
- Connect the discrete detectors/switches while the terminal module is attached to the sensor module.
- Connect the discrete detectors/switches while the terminal module is separated from the sensor module.

To make connections when the terminal module is attached:

1. Strip the insulation around 12mm from the end of each wire of discrete detectors/switches.
2. Fully insert each wire of both detectors/switches into each termination point.
   - Plug both wires of a detector/switch into the two termination points to the left.
   - Plug both wires of the other detector/switch into the two termination points to the right.



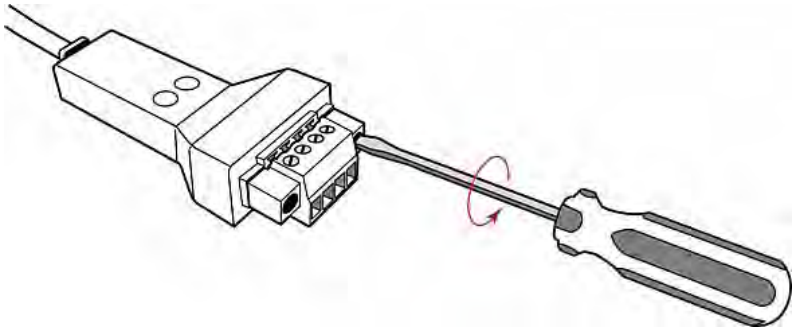
3. Use an appropriate screw driver to tighten the screws above each termination point until the connected wires are securely fastened.



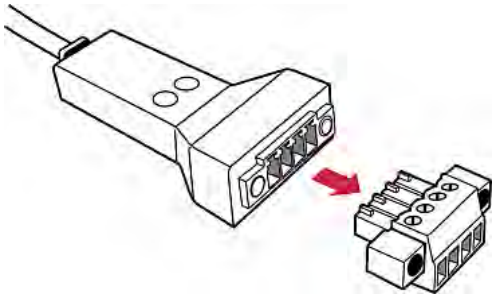
To make connections after the terminal module is separated:

1. Loosen the screws at two sides of the terminal module.

Note: The two screws are not removable so just loosen them.

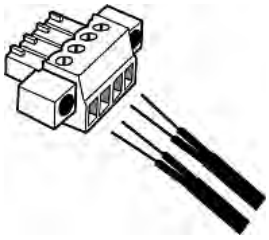


2. Separate the terminal module from the contact closure sensor.

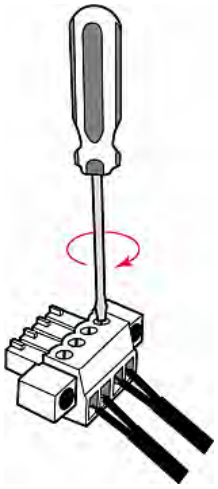


3. Strip the insulation around 12mm from the end of each wire of discrete detectors/switches.

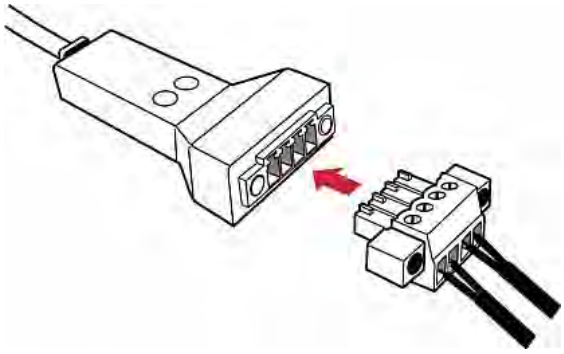
4. Fully insert each wire of both detectors/switches into each termination point.
   - Plug both wires of a detector/switch into the two termination points to the left.
   - Plug both wires of the other detector/switch into the two termination points to the right.



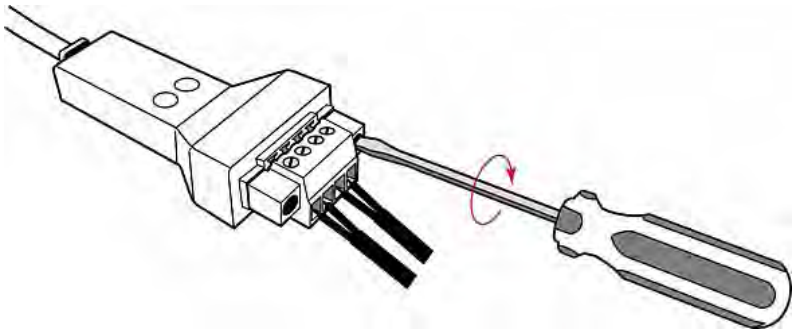
5. Use an appropriate screw driver to tighten the screws above each termination point until the connected wires are securely fastened.



6. Plug the terminal module back into the contact closure sensor.



7. Tighten the screws at two sides of the terminal module to secure it onto the contact closure sensor.

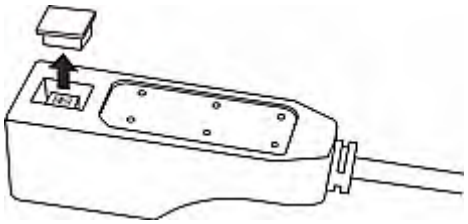


Configuring a Contact Closure Sensor

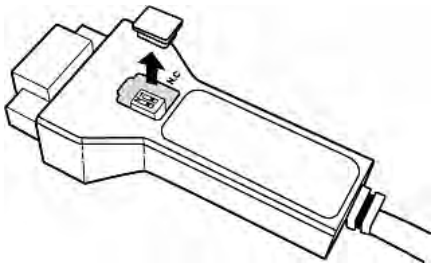
Before using DPX-CC2-TR to detect the contact closure status, water, smoke or vibration, you must determine the normal state by adjusting its dip switch, which controls the LED state on the body of DPX-CC2-TR. A dip switch is associated with a channel.

To adjust the dip switch setting:

1. Place the detectors/switches connected to DPX-CC2-TR to the position where you want to detect a specific environmental situation.
2. Uncover the dip switch on the body of DPX-CC2-TR.
   - **Old** DPX-CC2-TR



   - **New** DPX-CC2-TR

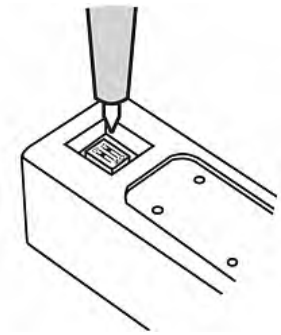


3. To set the Normal state for channel 1, locate the dip switch labeled 1.
4. Use a pointed tip such as a pen to move the slide switch to the end labeled N.O or N.C.

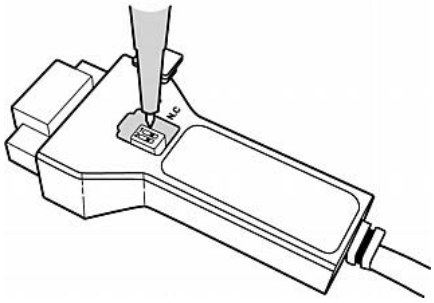
- N.O (Normally Open): The open status of the connected detector/switch is considered normal. This is the default.
- N.C (Normally Closed): The closed status of the connected detector/switch is considered normal.

For Raritan's water sensors, the Normal state should be Normally Open, which indicates there is no water detected. Adjust the dip switch setting to Normally Open and verify that the LED of the channel where the Raritan's water sensor is connected remains OFF.

- **Old** DPX-CC2-TR



- **New** DPX-CC2-TR



5. To set the Normal state for channel 2, repeat Step 4 for adjusting the other dip switch's setting.
6. Install back the dip switch cover.

Note: The dip switch setting must be properly configured, or the sensor LED may be incorrectly lit in the Normal state.

Contact Closure Sensor LEDs

DPX-CC2-TR has LEDs for showing the state of the connected detectors/switches.

The LED is lit when the associated detector/switch is in the "abnormal" state, which is the opposite of the Normal state. See ***Configuring a Contact Closure Sensor*** (on page 41) for how to set the Normal state.

The meaning of a lit LED varies depending on the Normal state settings.

- **When the Normal state is set to Normally Closed (N.C):**

LED	Sensor state
Not lit	Closed
Lit	Open

- **When the Normal state is set to Normally Open (N.O):**

LED	Sensor state
Not lit	Open
Lit	Closed

For Raritan's water sensors, the Normal state must be set to Normally Open (N.O). The following is the correct LED behavior based on proper dip switch settings.

LED	Sensor state
Not lit	No water detected
Lit	Water detected

Floor Water Sensors

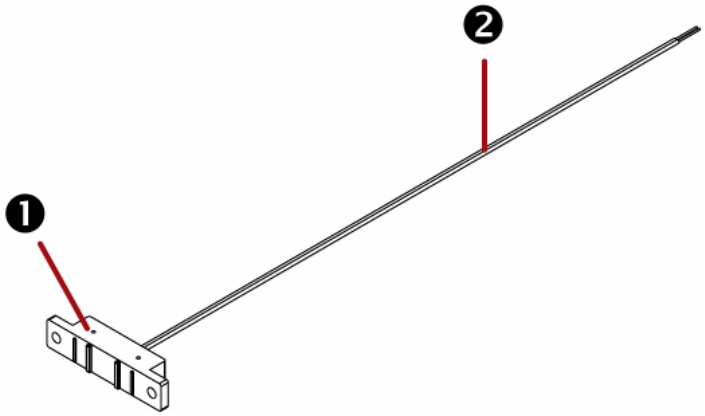
Raritan has two types of floor water sensors that can work in conjunction with Raritan's contact closure sensor. One is the floor-mounted water sensor, and the other is the cable water sensor.

- Floor-mounted water sensor (DPX-WSF):

  This detector has a flat bottom so it can stand on the ground. The dimension of the detector is 63.5 mm x 13.25 mm x 13.2 mm (W x L x D).

  Use either of the following ways to affix this detector onto the ground:

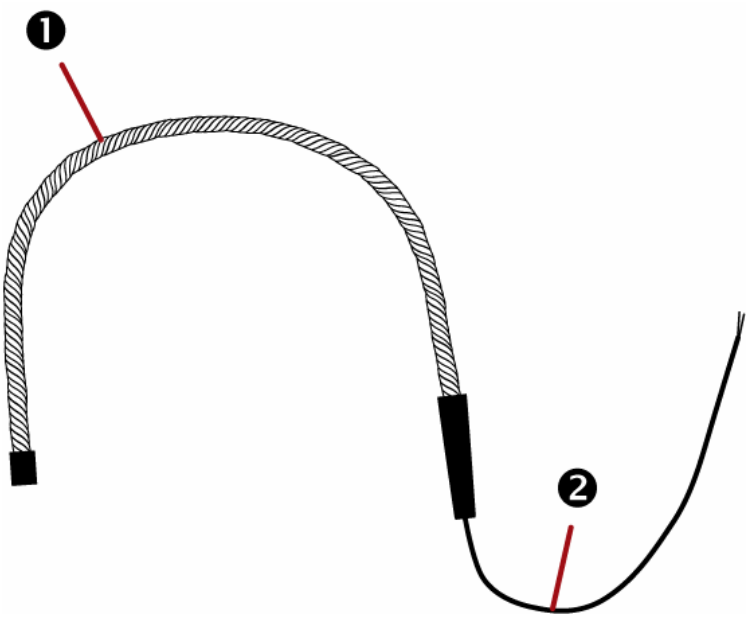
- Screw up the detector against the ground with your own screws. Do not over tighten the screws to avoid breaking the enclosure of the detector.
- Put something weighing around 100 through 250 grams into the empty bag shipped with this water sensor. Then use cable ties to wrap the bag right above the detector. Make sure the detector is not tilted so that its bottom evenly contacts the ground.



Number	Item
❶	Water detector.
❷	Wires to connect to Raritan's contact closure sensor. You need a minimum of 30 cm wires to prevent the contact closure sensor from being damaged by floor water (if any). Below are the wire length limitations: • Minimum: 30 cm • Maximum: 150 cm

- Cable water sensor (DPX-WSC series):

  This detector is in the shape of a cable so it can be flexibly placed, twisted or wrapped around a location where water may drip, such as a ceiling tile, water pipe or the floor. Depending on the type of the cable water sensor you purchased, the cable-shaped detector is either 3.5 or 7 meters long so its water detection area is longer than the floor-mounted water sensor.



Number	Item
❶	Cable-shaped water detector.
❷	Wires to connect to Raritan's contact closure sensor. You need a minimum of 30 cm wires to prevent the contact closure sensor from being damaged by floor water (if any). Below are the wire length limitations: • Minimum: 30 cm • Maximum: 150 cm

Differential Air Pressure Sensors

You can have a Raritan differential air pressure sensor connected to the PX device if the differential air pressure data is desired.

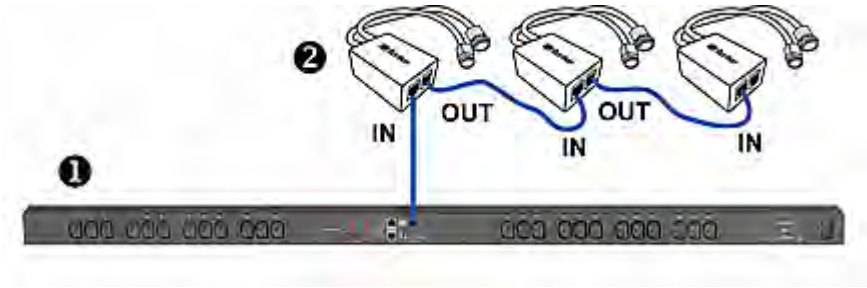
With this sensor, the temperature around the sensor can be also detected through a temperature sensor implemented inside it.

Multiple differential air pressure sensors can be cascaded.

To connect differential air pressure sensors:

1. Plug one end of a Raritan-provided phone cable to the SENSOR port of the PX device.
2. Plug the other end of this phone cable to the IN port of the differential air pressure sensor.
3. To connect additional Raritan differential air pressure sensors, do the following:
   a. Plug one end of a Raritan-provided phone cable to the OUT port of the previous differential air pressure sensor.
   b. Plug the other end of this phone cable to the IN port of the newly-added differential air pressure sensor.
   c. Repeat Steps a to b to cascade more differential air pressure sensors. Note that a SENSOR port supports a maximum of 16 environmental sensors.

❶	The PX device
❷	The Raritan differential air pressure sensor



Connecting the Asset Management Sensor (Optional)

You can remotely track the locations of up to 64 IT devices in the rack by connecting an asset management sensor (asset sensor) to the PX after these IT devices are tagged electronically.

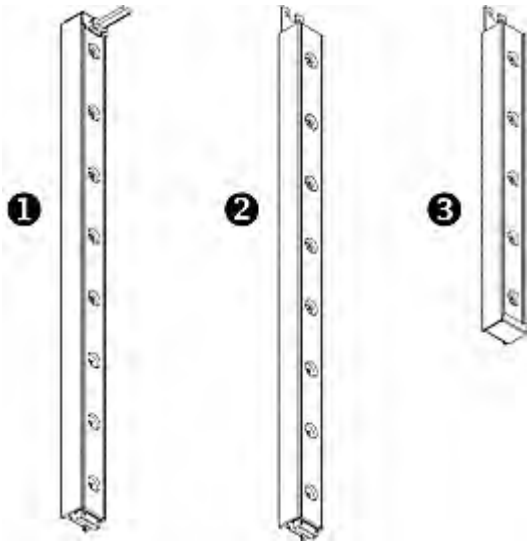
To use this asset management feature, you need the following items:

- Raritan asset sensors: An asset sensor transmits the tagging and positioning information to the PX.
- Raritan asset tags: An asset tag electronically tags the IT device where it is attached.

Combining Asset Sensors

Each tag port on the asset sensors corresponds to a rack unit and can be used to locate the IT devices on a specific rack (or cabinet). For each rack, you can attach asset sensors up to 64U long, consisting of one MASTER and multiple SLAVE asset sensors. The difference between the master and slave asset sensors is that the master asset sensor has an RJ-45 connector while the slave one does not.

The following diagram illustrates some asset sensors. Note that Raritan provides more types of asset sensors than the diagram.

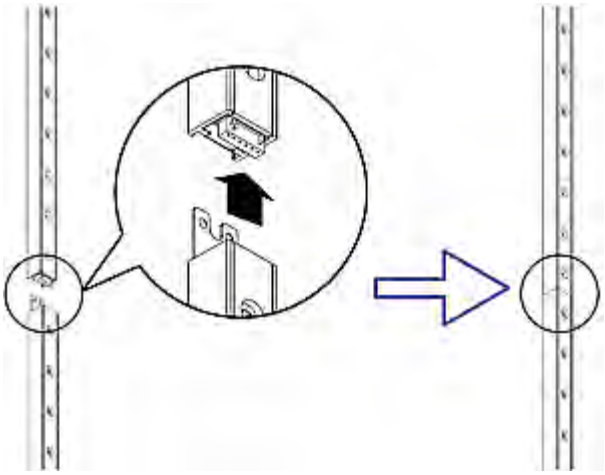


Number	Item
❶	8U MASTER asset sensor with 8 tag ports
❷	8U SLAVE asset sensor with 8 tag ports
❸	5U "ending" SLAVE asset sensor with 5 tag ports

Note: Unlike regular slave asset sensors, which have one DIN connector respectively on either end, the ending slave asset sensor has one DIN connector on only one end. An ending asset sensor is installed at the end of the asset sensor assembly.

To assemble asset sensors:

1. Connect a MASTER asset sensor to an 8U SLAVE asset sensor.
   - Plug the white male DIN connector of the slave asset sensor into the white female DIN connector of the master asset sensor.
   - Make sure that the U-shaped sheet metal adjacent to the male DIN connector is inserted into the rear slot of the master asset sensor. Screw up the U-shaped sheet metal to reinforce the connection.



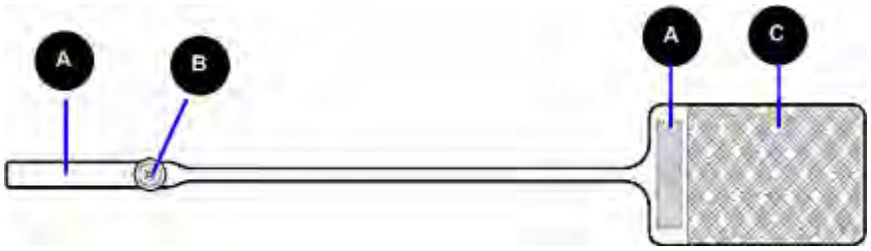
2. Connect another 8U slave asset sensor to the one being attached to the master asset sensor in the same manner as Step 1.
3. Repeat the above step to connect more slave asset sensors. The length of the asset sensor assembly can be up to 64U.
   - The final asset sensor can be 8U or 5U, depending on the actual height of your rack.
   - Using the "ending" asset sensor as the final asset sensor is strongly recommended.
4. Vertically attach the asset sensor assembly to the rack, next to the IT equipment, making each tag port horizontally align with a rack unit. The asset sensors are automatically attracted to the rack because of magnetic stripes on the back.

Note: The asset sensor is implemented with a tilt sensor so it can be mounted upside down.

Connecting Asset Sensors to the PX

You need both asset sensors and asset tags for tracking devices. Asset tags, which are adhered to devices, provide an ID number for each device, while the asset sensors transmit ID numbers and positioning information to the connected PX device.

The following diagram illustrates an asset tag.



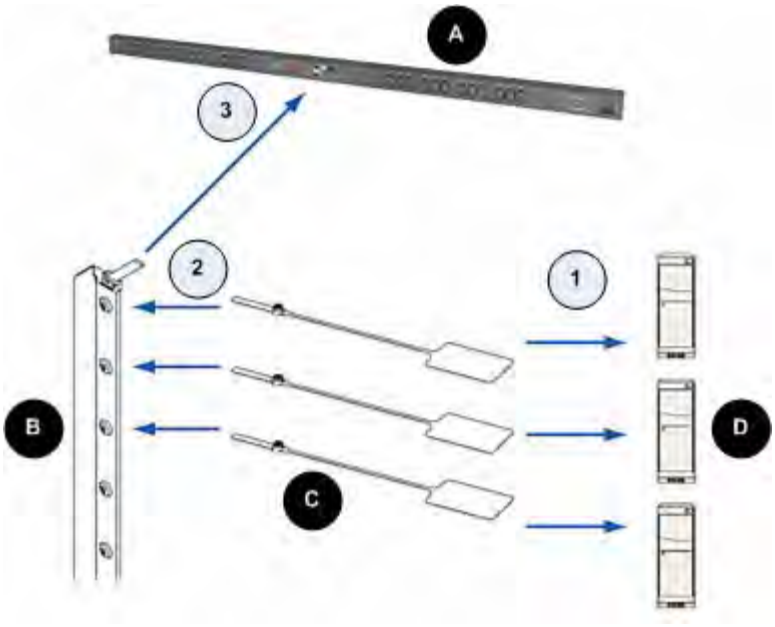
Letter	Item
A	Barcode (ID number), which is available on either end of the asset tag
B	Tag connector
C	Adhesive area with the tape

Note: The barcode of each asset tag is unique and is displayed in the PX web interface so it can easily be identified.

To connect asset sensors to the PX device:

1. Affix the adhesive end of an asset tag to each IT device through the tag's tape.
2. Plug the connector on the other end of each asset tag into the corresponding tag port on the asset sensor.
3. Connect the asset sensor assembly on the rack to the PX device.
   a. Connect one end of the Category 5e/6 cable to the RJ-45 connector on the MASTER asset sensor.
   b. Connect the other end of the cable to the FEATURE port on the PX device.

The PX device supplies power to the asset sensor assembly through the Category 5e/6 cable. All LEDs on the asset sensor assembly may cycle through different colors during the power-on process if the asset sensor's firmware is being upgraded by the PX device. After the power-on or firmware upgrade process completes, the LEDs show solid colors. Note that the LED color of the tag ports with asset tags connected will be different from the LED color of the tag ports without asset tags connected.



Letter	Item
A	The PX device
B	Asset sensors
C	Asset tags
D	IT devices, such as servers

Note: The PX cannot detect how many rack units the connected asset sensor(s) has. You must provide the information to it manually. See **Configuring the Asset Sensor** *(on page 233).*

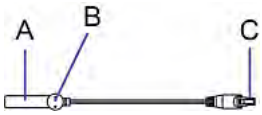
Connecting Blade Extension Strips

For blade servers, which are contained in a single chassis, you can use a blade extension strip to track individual blade servers.

Raritan's blade extension strip functions similar to a Raritan asset sensor but requires a tag connector cable for connecting to a tag port on the regular asset sensor or AMS-M2-Z. The blade extension strip contains 4 to 16 tag ports, depending on which model you purchased.

The diagram illustrates a tag connector cable and a blade extension strip with 16 tag ports.

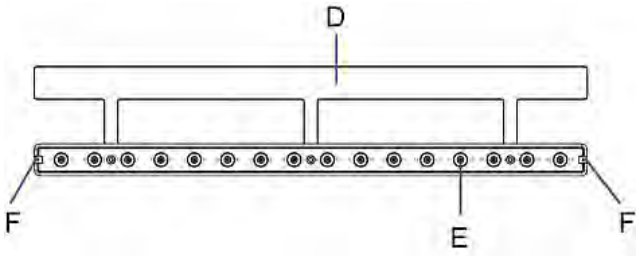
Tag connector cable



Item	Description
A	Barcode (ID number) for the tag connector cable
B	Tag connector
C	Cable connector for connecting the blade extension strip

Note: A tag connector cable has a unique barcode, which is displayed in the PX's web interface for identifying each blade extension strip where it is connected.

Blade extension strip

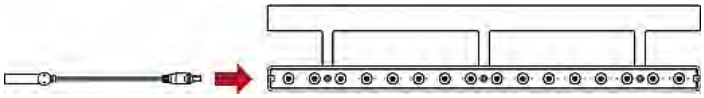


Item	Description
D	Mylar section with the adhesive tape
E	Tag ports
F	Cable socket(s) for connecting the tag connector cable

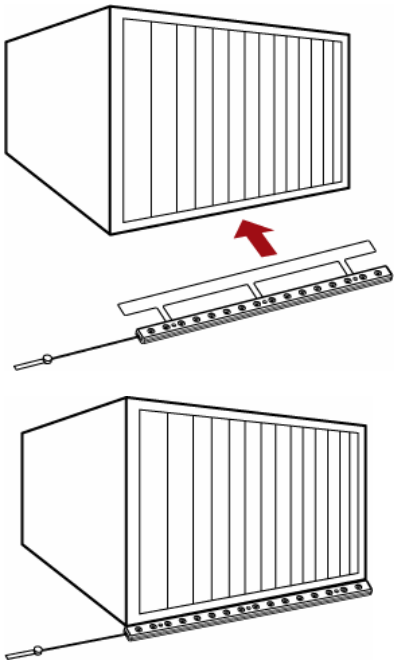
Note: Each tag port on the blade extension strip is labeled a number, which is displayed as the slot number in the PX's web interface.

To install a blade extension strip:

1. Connect the tag connector cable to the blade extension strip.
   - Plug the cable's connector into the socket at either end of the blade extension strip.

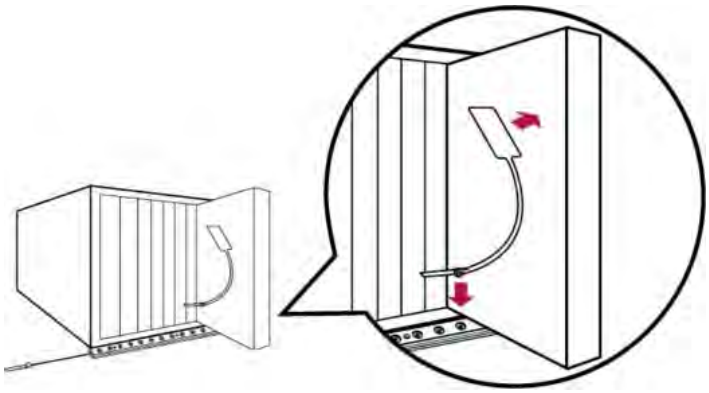


2. Move the blade extension strip toward the bottom of the blade chassis until its mylar section is fully under the chassis, and verify that the blade extension strip does not fall off easily. If necessary, you may use the adhesive tape in the back of the mylar section to help fix the strip in place.

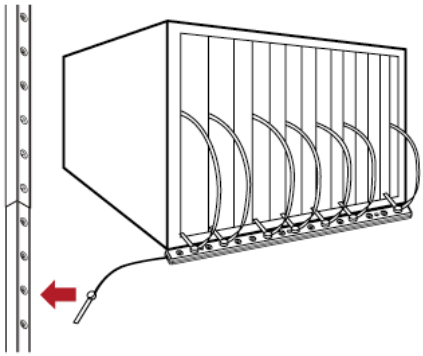


3. Connect one end of an asset tag to a blade server and connect the other end to the blade extension strip.
   a. Affix the adhesive part of the asset tag to one side of a blade server through the tag's tape.

b. Plug the tag connector of the asset tag into the tag port on the blade extension strip.



4. Repeat the above step until all blade servers in the chassis are connected to the blade extension strip via asset tags.
5. Plug the tag connector of the blade extension strip into the closest tag port of the asset sensor assembly or the AMS-M2-Z asset sensor on the rack.



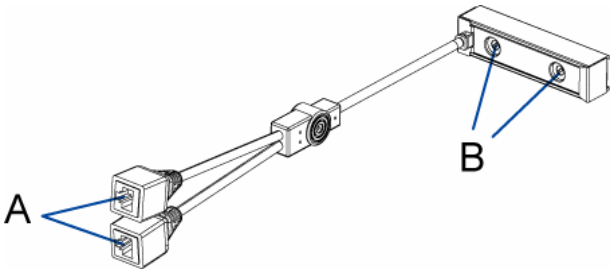
Note: If you need to temporarily disconnect the tag connector of the blade extension strip, wait at least 1 second before connecting it back, or the PX may not detect it.

Connecting AMS-M2-Z Asset Sensors (Optional)

The AMS-M2-Z is a special type of asset sensor that functions the same as regular MASTER asset sensors with the following differences:

- It provides two RJ-45 connectors
- Multiple AMS-M2-Z asset sensors can be daisy chained
- Only two tag ports are available on each AMS-M2-Z so only two asset tags can be connected

This product is especially useful for tracking large devices such as SAN boxes in the cabinet.



Item	Description
A	RJ-45 connectors
B	Tag ports

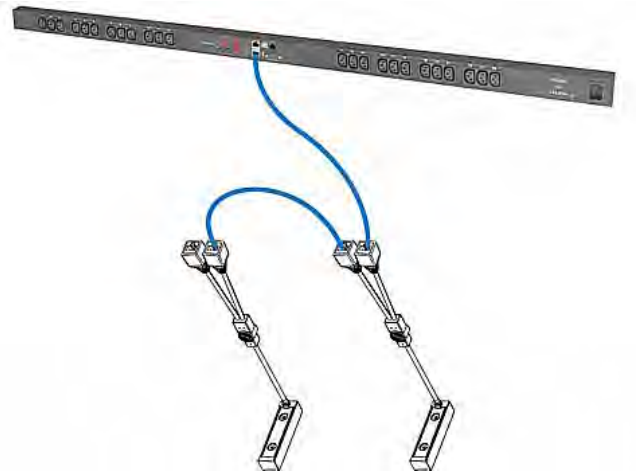
To connect the AMS-M2-Z asset sensors to the PX:

1. Connect the AMS-M2-Z to the PX via a Category 5e/6 cable.
   a. Connect one end of the cable to the RJ-45 port labeled "Input" on the AMS-M2-Z.
   b. Connect the other end of the cable to the FEATURE port on the PX.
2. Affix an asset tag to the IT device and connect this asset tag to the AMS-M2-Z by plugging the tag connector into the tag port on the AMS-M2-Z. See ***Connecting Asset Sensors to the PX*** (on page 49) for details.
3. If necessary, daisy chain multiple AMS-M2-Z to track more than two IT devices via this PX.
   a. Verify that the Category 5e/6 cable length is within the limitation. See ***AMS-M2-Z Daisy-Chain Limitations*** (on page 55) for the cable length limitations.
   b. Connect one end of the Category 5e/6 cable to the RJ-45 connector labeled "Output" on the AMS-M2-Z being connected to the PX.

c. Connect the other end of the cable to the RJ-45 connector labeled "Input" on another AMS-M2-Z.

d. Repeat the above steps to daisy chain additional AMS-M2-Z. See ***AMS-M2-Z Daisy-Chain Limitations*** (on page 55) for the maximum number of AMS-M2-Z asset sensors supported in the chain.

e. It is highly recommended using the cable ties to help hold the weight of all connecting cables.



4. Repeat Step 2 to connect IT devices to the other AMS-M2-Z's in the chain via the asset tags.

AMS-M2-Z Daisy-Chain Limitations

There are some limitations when daisy chaining the AMS-M2-Z asset sensors. The limitations vary according to the Raritan product model connected to the first AMS-M2-Z.

Models	Daisy-chain limitations
All PDUs whose model names begin with PX2	• Up to 2 AMS-M2-Z can be daisy chained. • The maximum cable length between each AMS-M2-Z in the chain is 2 meters.
EMX2-111	• Up to 2 AMS-M2-Z can be daisy chained. • The maximum cable length between each AMS-M2-Z in the chain is 2 meters.
EMX2-888	• Up to 6 AMS-M2-Z can be daisy chained. • The maximum cable length between each AMS-M2-Z in the chain is 3 meters.

Tip: To increase the maximum number of AMS-M2-Z units to be daisy chained for PX2 PDUs or EMX2-111, you can use Raritan's X cable to strengthen the AMS-M2-Z signals in the chain. See **Using an X Cable** *(on page 56).*

Using an X Cable

For Raritan's PX and EMX2-111 products, the number of AMS-M2-Z units to be daisy chained is limited to a maximum of two units per chain. See ***AMS-M2-Z Daisy-Chain Limitations*** (on page 55). To break the daisy-chain limitation, use Raritan's X cable to connect AMS-M2-Z. The number of AMS-M2-Z units to be daisy chained can be expanded from two up to six units.

An X cable is a combination of RJ-45 connectors, Raritan-designed phone connector and sensor port. The X cable offers 12V voltage from the SENSOR port of the PX or EMX2-111 to the connected AMS-M2-Z units, enhancing the AMS-M2-Z signals.

Note: An X cable does not help enhance the AMS-M2-Z signals for Raritan's EMX2-888, so usually it is not necessary to use this cable with the EMX2-888.

To connect AMS-M2-Z units via an X cable:

1. Plug the RJ-45 connector at the shorter end of the X cable into the FEATURE port of the PX device.

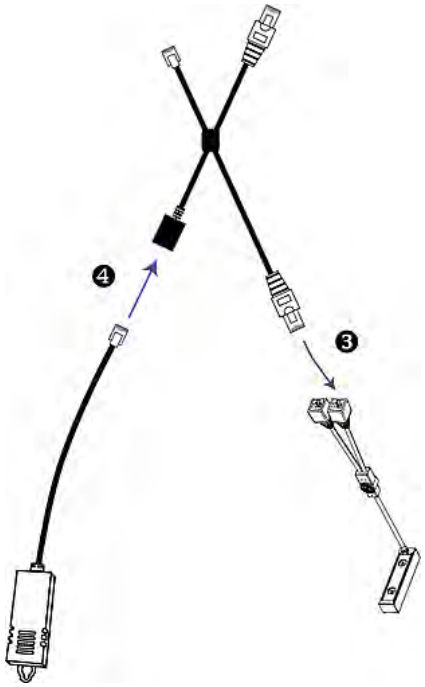
2. Plug the phone connector of the X cable into the SENSOR port of the PX device. **This step is required for improving the AMS-M2-Z signal strength.**

3. Plug the RJ-45 connector at the longer end of the X cable into the RJ-45 port labeled "Input" on the AMS-M2-Z.

Note: Though the X cable can also connect to a regular asset sensor, usually it is not necessary to make such a connection.

- A maximum of 5 additional AMS-M2-Z units can be connected to the AMS-M2-Z unit being attached to the X cable. See ***Connecting AMS-M2-Z Asset Sensors (Optional)*** (on page 54) for step-by-step instructions.

4. Connect any Raritan environmental sensor or hub to the sensor port of the X cable if you want to monitor environmental factors. See ***Connecting Environmental Sensors (Optional)*** (on page 33) for information on environmental sensors.



Connecting a Logitech Webcam (Optional)

The PX supports webcams connected to it, allowing you to view video or snapshots of the area surrounding the webcam. The following webcams are supported:

- Logitech® Webcam® Pro 9000, Model 960-000048
- Logitech QuickCam Deluxe for Notebooks, Model 960-000043
- Logitech QuickCam Communicate MP, Model 960-000240
- Logitech C200

The PX supports up to one webcam. After connecting a webcam, you can visually monitor environmental conditions near the PX through the web interface from anywhere.

For more information on the Logitech webcam, see the user documentation accompanying it.

To connect a webcam:

1. Connect the webcam to the USB-A port on the PX device. The PX automatically detects the webcam.

2. Position the webcam properly.

Snapshots or videos captured by the webcam are immediately displayed in the PX web interface. See ***Viewing the Webcam Snapshots or Videos*** (on page 243).

Connecting a GSM Modem (Optional)

A Cinterion® MC52iT or MC55iT GSM modem must be connected to the PX in order to send SMS event messages. See ***Creating Actions*** (on page 181) for more information on SMS event messages.

Note: The PX cannot receive SMS messages.

To connect the GSM modem:

1. Connect the GSM modem to the DB9 serial port on the PX.
2. Configure the GSM modem as needed. See the supporting GSM modem help for information on configuring the GSM modem.
3. Configure the GSM modem settings in PX.
   a. Click Device Settings > Serial Port Settings. The Serial Port Configuration dialog opens.
   b. If needed, enter the GSM modem SIM PIN.

Connecting a Schroff LHX Heat Exchanger (Optional)

To remotely monitor and administer the Schroff® LHX-20 or LHX-40 heat exchangers through the PX device, you must establish a connection between the heat exchanger and the PX device. Note that only the PDUs whose model names begin with PX2 support the LHX heat exchangers.

For more information on the LHX heat exchanger, see the user documentation accompanying that product.

To establish a connection between the PDU and LHX heat exchanger, an RJ-45 to RS-232 adapter cable provided by Schroff is required.

To connect an LHX heat exchanger:

1. Plug the RS-232 DB9 end of the adapter cable into the RS-232 port on the Schroff LHX heat exchanger.
2. Plug the RJ-45 end of the cable into the port labeled FEATURE on your PX device.

See ***Managing the Schroff LHX Heat Exchanger*** (on page 251) for enabling the support of the LHX heat exchanger.

Connecting an RF Code PDU Sensor Tag (Optional)

If you have the RF Code R170 PDU sensor tag, you can have the power data of the PX sent to the RF Code management software for monitoring the energy utilization status. See ***RF Code Energy Monitoring Solution*** (on page 495) for more information.

To send the power data of the PX to RF Code software:

- Plug an RF Code R170 PDU sensor tag into the SENSOR port of the PX.

Chapter 5 Using the PDU

This chapter explains how to use the PX device. It describes the LEDs and ports on the PDU, and explains how to use the LED display panel. It also explains how the circuit breaker (overcurrent protector) works and when the beeper sounds.

In This Chapter

Panel Components 61
Circuit Breakers 71
Fuse 73
Beeper 76

Panel Components

The PX comes in Zero U, 1U, and 2U sizes. All types of models come with the following components on the outer panels.

- Power cord
- Outlets
- Connection ports
- LED display
- Reset button

Power Cord

Most of Raritan PDUs come with an installed power cord, which is ready to be plugged into an appropriate receptacle for receiving electricity. Such devices cannot be rewired by the user.

Connect each PX device to an appropriately rated branch circuit. See the label or nameplate affixed to your PX device for appropriate input ratings or range of ratings.

There is no power switch on the PX device. To power cycle the PDU, unplug it from the branch circuit, wait 10 seconds and then plug it back in.

Outlets

The total number of outlets varies from model to model.

PX2-3000 Series

These PDUs are NOT outlet-switching capable models so all outlets are always in the ON state.

Outlet LEDs are not available.

PX2-4000 Series

These PDUs are NOT outlet-switching capable models so all outlets are always in the ON state.

A small LED is adjacent to each outlet to indicate the outlet state. Outlet LEDs always light red, indicating that the outlet power is ON.

PX2-5000 Series

These models are outlet-switching capable PDUs. A small LED is adjacent to each outlet to indicate the outlet or PDU state. The PDU is shipped from the factory with all outlets turned ON. The table below explains how to interpret different outlet LED states.

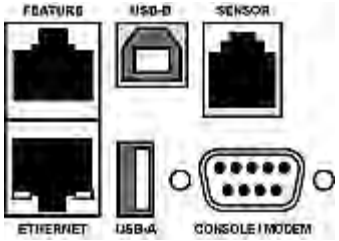
LED state	Outlet status	What it means
Not lit	Powered OFF	The outlet is not connected to power, or the control circuitry's power supply is broken.
Red	ON and LIVE	LIVE power. The outlet is on and power is available.
Red flashing	ON and LIVE	The current flowing through the outlet is greater than the upper warning (non-critical) threshold.
Green	OFF and LIVE	The outlet is turned off and power is available when the outlet is turned on.
Green flashing	OFF and NOT LIVE	The outlet is turned off and power is not available because the circuit breaker has tripped.
Red and Green flashing alternatively	ON and NOT LIVE	The outlet is turned on but power is not available because a circuit breaker has tripped.
Cycling through Red, Green and Yellow	n/a	The PX device has just been plugged in and its management software is loading.

Note: When a PX device powers up, it proceeds with the power-on self test and software loading for a few moments. At this time, the outlet LEDs cycle through different colors. When the software has completed loading, the outlet LEDs show a steady color and the LED display illuminates.

Connection Ports

Depending on the model you purchased, the total number of ports available varies.

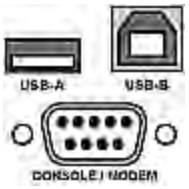
- For most of Zero U models, there are 6 ports located on the front panel as shown below.



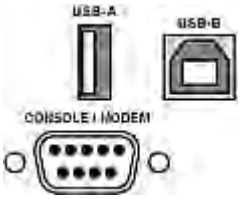
- For most of 1U and 2U models, there are 7 ports located on front and back panels respectively.

  - Front panel ports:

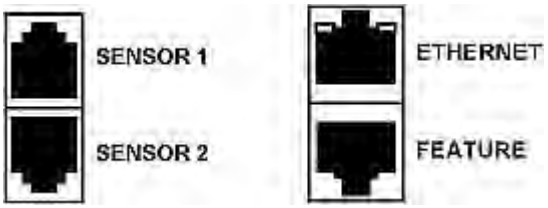
  1U



  2U



  - Back panel ports:



The only port difference between Zero U, 1U and 2U models is that Zero U models provide only one sensor port while 1U and 2U models provide two.

The table below explains the function of each port.

Port	Used for...
USB-B	Establishing a USB connection between a computer and the PX device. This port can be used for disaster recovery of the PX device. Contact Raritan Technical Support for instructions.

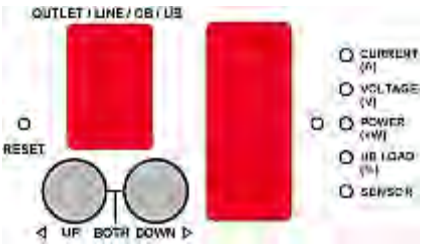
Port	Used for...
USB-A	Connecting a USB device, such as a Logitech® webcam. This is a "host" port, which is powered, per USB 2.0 specifications.
FEATURE	Connection to some Raritan access products (such as Dominion KX II) through the use of a power CIM, OR -- Connection to a Schroff® LHX-20 or LHX-40 device through a RJ-45 to RS-232 cable provided by Schroff, OR -- Connection to a Raritan asset management sensor, which allows you to track the locations of the IT devices on the rack. See ***Connecting the Asset Management Sensor (Optional)*** (on page 47). *Warning: This is not an RS-232 port so do NOT plug in an RS-232 device, or damages can be caused to the device.*
CONSOLE/ MODEM	Establishing a serial connection between a computer and the PX device: This is a standard DTE RS-232 port. You can use a null-modem cable with two DB9 connectors on both ends to connect the PX device to the computer.
SENSOR	Connection to Raritan's environmental sensors. For Zero U products, a sensor hub is required if you want to connect more than one environmental sensor.
ETHERNET	Connecting the PX device to your company's network: Connect a standard Cat5e/6 UTP cable to this port and connect the other end to your network. This connection is necessary to administer or access the PX device remotely using the web interface. There are two small LEDs adjacent to the port: ▪ Green indicates a physical link and activity. ▪ Yellow indicates communications at 10/100 BaseT speeds. For a USB-cascading configuration, the wired network connection is a must for the *master* PX. See ***Cascading the PX via USB*** (on page 29) for details. *Note: Connection to this port is not required if the PX device is connected to a wireless network.*

LED Display

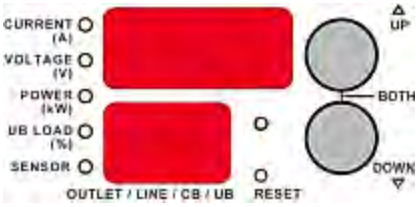
The LED display is located on the side where outlets are available.

These diagrams show the LED display on different types of PDUs. Note that the LED display might slightly vary according to the PDU you purchased.

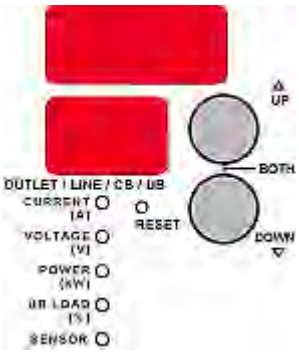
Zero U models:



1U models:



2U models:



The LED display consists of:

- A row displaying three digits
- A row displaying two digits
- Up and Down buttons
- Five LEDs for measurement units

A Zero U model can detect its own orientation through the built-in tilt sensor and automatically changes the direction of the alphanumeric digits shown on the LED display for easy reading. To lock the direction of the digits shown on the LED display, you can set the display orientation using the command line interface. See ***Changing the LED Display Orientation*** (on page 313).

Note: When a PX device powers up, it proceeds with the power-on self test and software loading for a few moments. When the software has completed loading, the LED display illuminates.

Three-Digit Row

The three-digit row shows the readings for the selected component. Values that may appear include:

- Current, voltage, or active power of the selected outlet
- Active power or unbalanced load of the inlet
- Current of the selected circuit breaker
- Current and voltage of the selected line

  Note: L1 voltage refers to the L1-L2 or L1-N voltage, L2 voltage refers to the L2-L3 or L2-N voltage, and L3 voltage refers to the L3-L1 or L3-N voltage.

- The text “FuP,” which indicates that the **F**irmware **uP**grade is being performed
- The text "CbE," which indicates the circuit breaker associated with the selected outlet has tripped

LEDs for Measurement Units

Five small LED indicators are on the LED display: four measurement units LEDs and one Sensor LED.

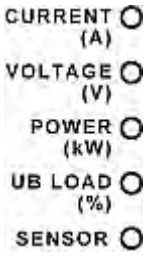
The measurement units vary according to the readings that appear in the three-digit row. They are:

- Amp (A) for current
- Volt (V) for voltage
- Kilowatt (kW) for active power
- Percentage (%) of the unbalanced load

One of the measurement unit LEDs will be lit to indicate the unit for the value currently shown in the three-digit row.

The Sensor LED is lit only when PX detects the physical connection of any environmental sensor.

The five LEDs look similar to this diagram but may slightly vary according to the model you purchased.



Two-Digit Row

The two-digit row shows the number of the currently selected outlet, line or circuit breaker. Values that may appear include:

- Two-digit numbers: This indicates the selected outlet. For example, 03 indicates outlet 3.
- Cx: This indicates the selected circuit breaker, where x is the circuit breaker number. For example, C1 represents Circuit Breaker 1.
- Lx: This indicates the selected line, where x is the line number. For example, L2 represents Line 2.

Note: For a single-phase model, L1 current represents the Unit Current.

- AP: This indicates the selected inlet's active power.
- UL: This represents the selected inlet or outlet's **U**nbalanced **L**oad, which is only available for a three-phase PDU.
- ix: This refers to the selected inlet on a multi-inlet PDU, where x is the inlet number. For example, `i1` refers to Inlet 1, and `i2` refers to Inlet 2.

  The two-digit row shows the inlet number while displaying an inlet's line or active power on a multi-inlet PDU. It will cycle through the selected inlet number and that inlet's line or active power (AP). For example, when cycling through i1 and L1, the value displayed in the three-digit row belongs to Inlet 1's L1, and when cycling through i2 and L1, the displayed value belongs to Inlet 2's L1.

  Note: The point of the alphabet 'i' cannot be displayed on the LED display so `i1` looks like ı 1 and `i2` looks like ı 2.

During the firmware upgrade, some PX models may show `bx` in the two-digit row to indicate the relay or meter board numbered x is being updated.

Automatic Mode

When left alone, the LED display cycles through the line readings and circuit breaker readings at intervals of 10 seconds, as available for your PX. This is the Automatic Mode.

For each line reading, the PX always displays `i1` for Inlet 1 or `i2` for Inlet 2 in the two-digit row of the LED display as described below:

- When showing L1 of Inlet 1, the two-digit row cycles through `i1` and `L1`.
- When showing L1 of Inlet 2, the two-digit row cycles through `i2` and `L1`.

Note: The point of the alphabet 'i' cannot be displayed on the LED display so `i1` looks like ı 1 and `i2` looks like ı 2.

Manual Mode

You can press the Up or Down button to enter the Manual Mode so that a particular outlet, line or circuit breaker can be selected to show specific readings.

In addition, you can select a particular inlet if your PDU has more than one inlet. Each inlet is indicated as `i1`, `i2`, or the like in the two-digit row of the LED display.

Note: The point of the alphabet 'i' cannot be displayed on the LED display so `i1` looks like ı 1 and `i2` looks like ı 2.

To operate the LED display:

1. Press the Up or Down button until the desired outlet, line or circuit breaker number is selected in the two-digit row. Or you can press either button to select the inlet's active power, which is shown as *AP*.
   - Pressing the △ (UP) button moves up one selection.
   - Pressing the ▽ (DOWN) button moves down one selection.

   If your PDU is a multi-inlet PDU and you select a specific inlet's line or active power (AP), the two-digit row will cycle through the selected inlet number and that inlet's line or active power. For example:
   - When showing L1 of Inlet 1, the two-digit row cycles through `i1` and `L1`.
   - When showing L1 of Inlet 2, the two-digit row cycles through `i2` and `L1`.
   - When showing active power of Inlet 1, the two-digit row cycles through `i1` and AP.
   - When showing active power of Inlet 2, the two-digit row cycles through `i2` and AP.
2. Current of the selected component is shown in the three-digit row. Simultaneously the CURRENT(A) LED is lit. See ***LEDs for Measurement Units*** (on page 67).
3. When selecting an outlet or a line, you can press the Up and Down buttons simultaneously to switch between voltage, active power and current readings.
   - When the voltage is displayed, the VOLTAGE(V) LED is lit. It is displayed for about five seconds, after which the current reading re-appears.
   - When the active power is displayed, the POWER(kW) LED is lit. It is displayed for about five seconds, after which the current reading re-appears.

4. When selecting AP, it displays the selected inlet's active power reading.
   - When the active power is displayed, the POWER(kW) LED is lit.

Note: The LED display returns to the Automatic Mode after 20 seconds elapse since the last time any button was pressed.

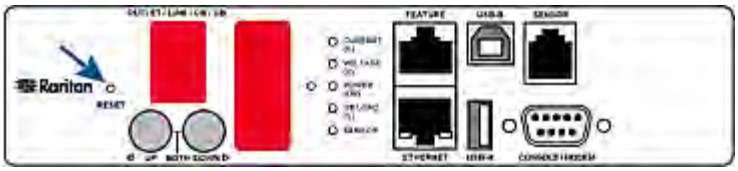
Reset Button

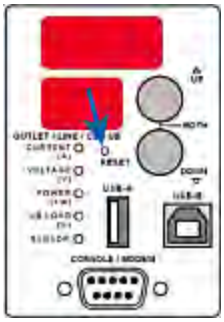
The reset button is located inside the small hole near the two-digit row.

The PX device can be reset to its factory default values using this button when a local connection is available. See ***Resetting to Factory Defaults*** (on page 467).

Without the serial connection, pressing this reset button restarts the PX device's software without any loss of power to outlets.

The following images indicate the locations of the reset button on 0U, 1U and 2U models.





Circuit Breakers

The PX models rated over 20A (North American) or 16A (international) contain branch circuit breakers. These circuit breakers automatically trip (disconnect power) when the current flowing through the circuit breaker exceeds its rating.

If the circuit breaker switches off power, the LED display shows:

- CbE, which means "circuit breaker error," in the three-digit row.
- The lowest outlet number affected by the circuit breaker error in the two-digit row.

You are still able to switch between outlets on the LED display when the circuit breaker error occurs. Outlets affected by the error show CbE. Unaffected outlets show the current and voltage readings as described in ***Manual Mode*** (on page 69).

When a circuit breaker trips, power flow ceases to all outlets connected to it. You must manually reset the circuit breaker so that affected outlets can resume normal operation.

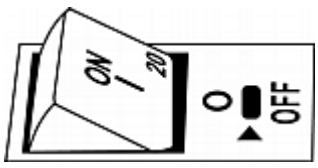
Depending on the model you purchased, the circuit breaker may use a button- or handle-reset mechanism.

Resetting the Button-Type Circuit Breaker

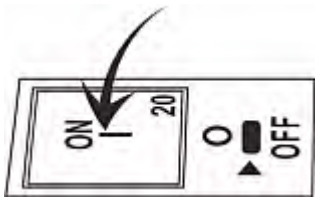
Your button-type circuit breakers may look slightly different from the images shown in this section, but the reset procedure remains the same.

To reset the button-type breakers:

1. Locate the breaker whose ON button is up, indicating the breaker has tripped.



2. Examine your PX device and the connected equipment to remove or resolve the cause that results in the overload or short circuit. **This step is required, or you cannot proceed with the next step.**
3. Press the ON button until it is completely down.

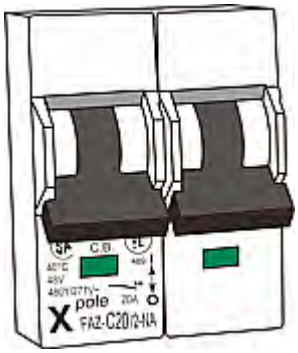


Resetting the Handle-Type Circuit Breaker

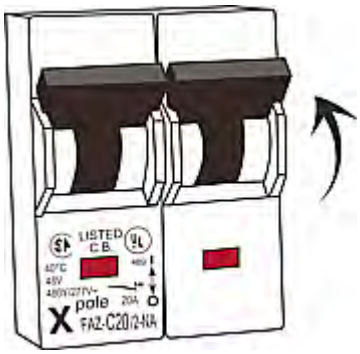
Your handle-type circuit breakers may look slightly different from the images shown in this section, but the reset procedure remains the same.

To reset the handle-type breakers:

1. Lift the hinged cover over the breaker.
2. Check if the colorful rectangle or triangle below the operating handle is GREEN, indicating the breaker has tripped.



3. Examine your PX device and the connected equipment to remove or resolve the cause that results in the overload or short circuit. **This step is required, or you cannot proceed with the next step.**
4. Pull up the operating handle until the colorful rectangle or triangle turns RED.



Fuse

Some PX devices are implemented with fuses instead of circuit breakers. A fuse blows to protect associated outlets if it detects the overload.

If your PDU uses fuses, you must replace it with a new one when it blows or malfunctions. The rating of the new fuse must be the same as the original one.

Use of inappropriately rated fuse results in damage to the PDU and connected equipment, electric shock, fire, personal injury or death.

Depending on the design of your PDU, the fuse replacement methods differ.

Fuse Replacement on Zero U Models

This section only applies to a Zero U PDU with "replaceable" fuses.

To replace a fuse on the Zero U model:

1. Lift the hinged cover over the fuse.

2. Verify the new fuse's rating against the rating specified in the fuse holder's cover.

3. Push the cover of the fuse holder to expose the fuse.

4. Take the fuse out of the holder.

5. Insert a new fuse into the holder. There is no orientation limit for fuse insertion.
6. Close the fuse holder and the hinged cover in a reverse order.

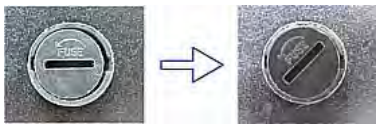
Fuse Replacement on 1U Models

On the 1U model, a fuse is installed in a fuse knob, which fits into the PDU's fuse carrier.

Number	Description
❶	Fuse carrier
❷	Fuse knob where a fuse is installed

To replace a fuse on the 1U PDUs:

1. Disconnect the PDU's power cord from the power source.
2. Remove the desired fuse from the PDU's fuse carrier using a flat screwdriver.
   a. Rotate the fuse knob counterclockwise until its slot is inclined to 45 degrees.



   b. Take this knob out of the fuse carrier.
3. Remove the original fuse from this knob, and insert either end of a new one into the knob. Make sure the new fuse's rating is the same as the original one.

Number	Description
❶	Fuse knob
❷	Fuse

4. Install this knob along with the new fuse into the fuse carrier using a flat screwdriver.
   a. Have this knob's slot inclined 45 degrees when inserting the knob into the fuse carrier.

   b. Gently push this knob into the fuse carrier and then rotate it clockwise until its slot is horizontal.

5. Verify whether this knob's head is aligned with the fuse carrier. If its head is higher or lower than the fuse carrier, re-install it.

Number	Description
❶	INAPPROPRIATE installations
❷	Appropriate installation

6. Connect the PDU's power cord to the power source and verify that the corresponding fuse LED is lit, indicating that the fuse works properly.

Beeper

The PX includes a beeper to issue an audible alarm when a significant situation occurs.

- The beeper sounds an alarm within 3 seconds of a circuit breaker trip.
- The beeper stops as soon as all circuit breakers have been reset.

Chapter 6 Using the Web Interface

This chapter explains how to use the web interface to administer a PX.

In This Chapter

Supported Web Browsers....77
Logging in to the Web Interface....78
Logout....80
Introduction to the Web Interface....81
Viewing the Dashboard....93
Device Management....94
User Management....119
Setting Up Roles....125
Access Security Control....128
Setting Up an SSL Certificate....142
Setting Up External Authentication....147
Outlet Management....155
Inlet and Circuit Breaker Management....170
Setting Power Thresholds....173
Event Rules and Actions....180
Managing Event Logging....215
Viewing Connected Users....216
Monitoring Server Accessibility....217
Environmental Sensors....221
Asset Management....232
Bulk Configuration....238
Backup and Restore of PX Device Settings....240
Webcam Management....242
Network Diagnostics....248
Viewing the Communication Log....249
Downloading Diagnostic Information....250
Managing the Schroff LHX Heat Exchanger....251
Firmware Upgrade....258
Accessing the Help....261

Supported Web Browsers

The following web browsers can be used to access the PX web interface based on the firmware version 2.4:

- Internet Explorer® 8 and 9
- Firefox® 10+
- Safari® 5.x (MacOS Lion)
- Google® Chrome® 12+ and 17+
- Android 3+ (standard browser)
- IOS 5.0 (for both iPhone and iPad)

Logging in to the Web Interface

To log in to the web interface, you must enter a user name and password. The first time you log in to the PX, use the default user name (admin) and password (raritan). You are then prompted to change the password for security purposes.

Exception: If you already changed the password for the admin account during the **Initial Network Configuration** *(on page 22), use the new password instead to log in to the web interface, and the PX will NOT prompt you to change the password.*

After successfully logging in, you can create user profiles for your other users. These profiles define their login names and passwords. See ***Creating a User Profile*** (on page 120).

Login

The web interface allows a maximum of 16 users to log in simultaneously.

You must enable JavaScript in the web browser for proper operation.

▶ **To log in to the web interface:**

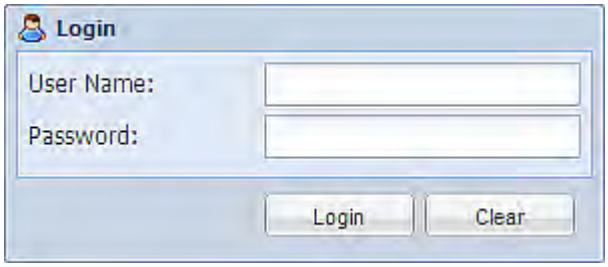
1. Open a browser, such as Microsoft Internet Explorer or Mozilla Firefox, and type this URL:

   http(s)://<ip address>

   where *<ip address>* is the IP address of the PX device.

2. If a security alert message appears, click OK or Yes to accept. The Login page then opens.

3. Type your user name in the User Name field, and password in the Password field.



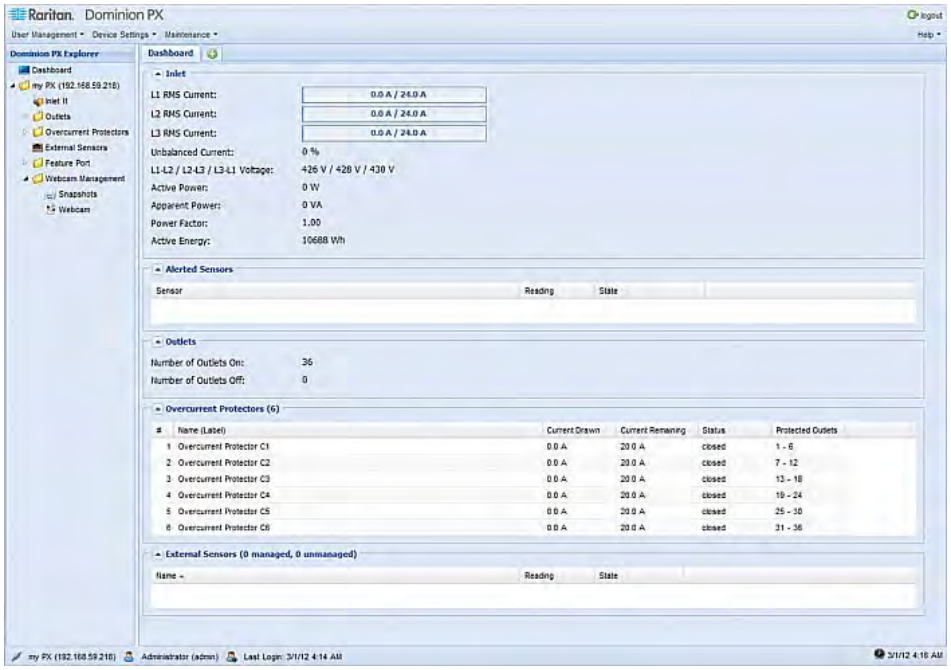
Note: Both the user name and password are case sensitive, so make sure you capitalize them correctly. Click Clear to clear either the inputs or any error message that appears.

4. If a security agreement is displayed on the Login page, accept it.

Note: If you do not accept the security agreement, you cannot log on to the PX.

5. Click Login or press Enter. The PX page opens.

Note: Depending on your hardware configuration, elements shown on the PX page may appear slightly different from this image.


Raritan. Dominion PX
User Management
Device Settings
Maintenance
Help
Logout
Dominion PX Explorer
Dashboard
my PX (192.168.59.216)
Inlet II
Outlets
Overcurrent Protectors
External Sensors
Feature Port
Webcam Management
Snapshots
Webcam
Inlet
L1 RMS Current: 0.0 A / 24.0 A
L2 RMS Current: 0.0 A / 24.0 A
L3 RMS Current: 0.0 A / 24.0 A
Unbalanced Current: 0 %
L1-L2 / L2-L3 / L3-L1 Voltage: 426 V / 428 V / 430 V
Active Power: 0 W
Apparent Power: 0 VA
Power Factor: 1.00
Active Energy: 10688 Wh
Alerted Sensors
Sensor
Reading
State
Outlets
Number of Outlets On: 36
Number of Outlets Off: 0
Overcurrent Protectors (6)
Name (Label) Current Drawn Current Remaining Status Protected Outlets
1 Overcurrent Protector C1 0.0 A 20.0 A closed 1 - 6
2 Overcurrent Protector C2 0.0 A 20.0 A closed 7 - 12
3 Overcurrent Protector C3 0.0 A 20.0 A closed 13 - 18
4 Overcurrent Protector C4 0.0 A 20.0 A closed 19 - 24
5 Overcurrent Protector C5 0.0 A 20.0 A closed 25 - 30
6 Overcurrent Protector C6 0.0 A 20.0 A closed 31 - 36
External Sensors (0 managed, 0 unmanaged)
Name
Reading
State
my PX (192.168.59.216)
Administrator (admin)
Last Login: 3/1/12 4:14 AM
3/1/12 4:16 AM

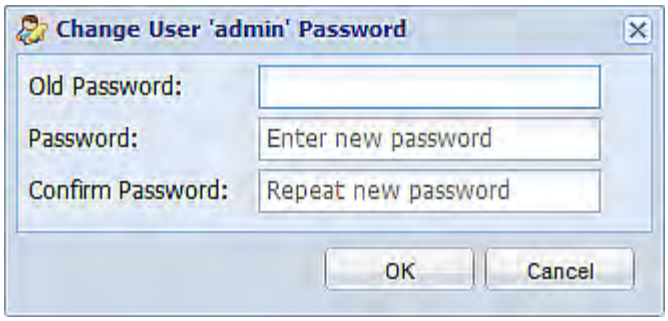
Changing Your Password

Normal users can change their own passwords if they have the Change Own Password permission. See ***Setting Up Roles*** (on page 125).

If you are the administrator (admin), the PX web interface automatically prompts you to change the password if this is your first time to log in to the PX. If you have the Administrator Privileges, you can change other users' passwords, as well. See ***Modifying a User Profile*** (on page 123).

To change your password:

1. Choose User Management > Change Password. The Change User Password dialog appears.



2. Type the current password in the Old Password field.
3. Type your new password in the Password and Confirm Password fields. The password can be 4 to 32 characters long. It is case sensitive.
4. Click OK to save the changes.

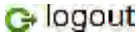
Tip: If you have the Administrator Privileges, you can change other users' passwords. See **Modifying a User Profile** *(on page 123).*

Logout

After finishing your tasks with the PX, you should log out to prevent others from accessing the web interface.

To log out of the web interface:

1. Do one of these:
   - Click "logout" on the top-right corner of the web interface.

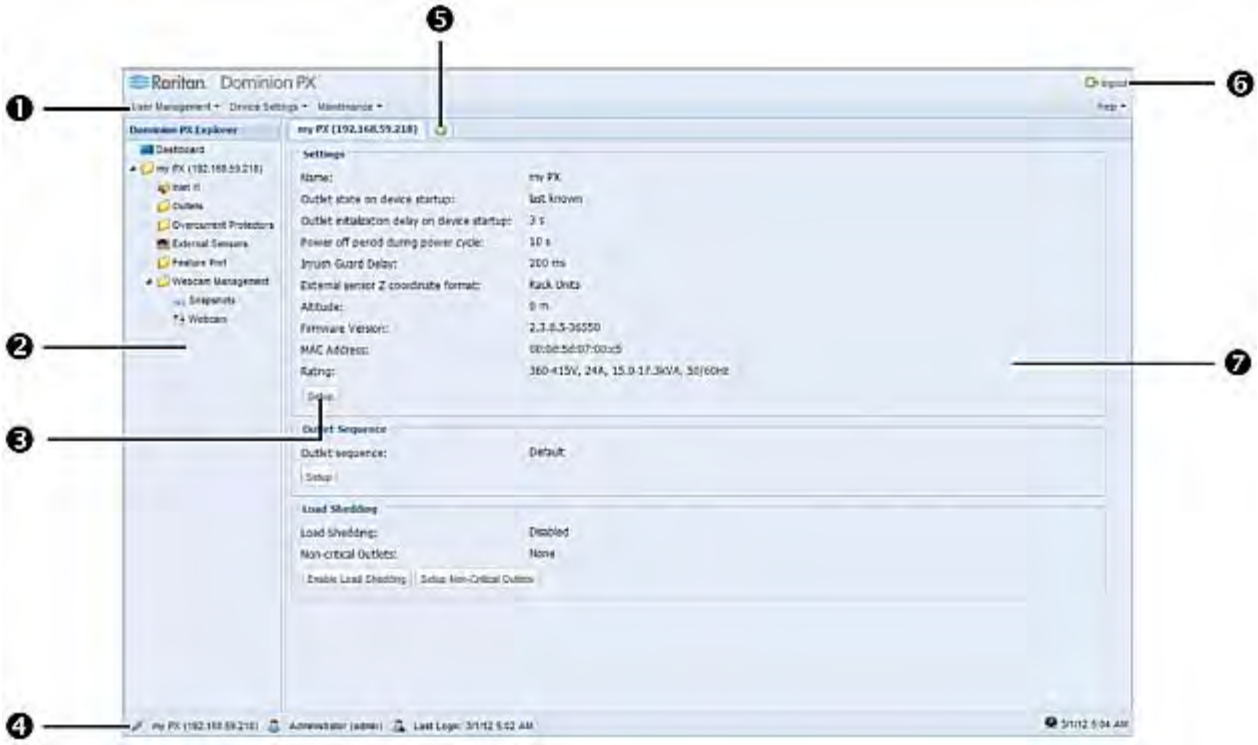
   - Close the web browser by clicking the Close button ( ) on the top-right corner of the browser.

- Close the web browser by choosing File > Close, or File > Exit. The command varies according to the version of the browser you use.
- Choose the Refresh command or click the Refresh button on the web browser.

2. Either the login page opens or the browser is closed, depending on your choice in the previous step.

Introduction to the Web Interface

The web interface provides two panes, a menu bar, a status bar, an Add Page icon, and a logout button throughout every page.



Number	Web interface element
❶	Menus
❷	Dominion PX Explorer pane
❸	Setup button*
❹	Status bar
❺	Add Page icon
❻	Logout button

Number	Web interface element
❼	Data pane

* The Setup button is not available on some pages, such as the *Dashboard* page.

For detailed information about these web interface elements, see the sections that follow.

Menus

There is a menu bar across the top of the page. You can click any menu to select the desired menu item from the drop-down list.

Four menus are available for managing different tasks or showing information.

- **User Management** contains menu items for managing user profiles, permissions (roles), and password.
- **Device Settings** deals with device-related settings, such as the device name, network settings, security settings, and system time.
- **Maintenance** provides tools that are helpful for maintaining the PX, such as the event log, hardware information, firmware upgrade and so on.
- **Help** displays information regarding the firmware and all open source packages embedded on the PX. In addition, you can access the user guide from this menu.

Dominion PX Explorer Pane

The hierarchical tree to the left displays the PX device you are accessing as well as all physical components embedded on or connected to this PDU, such as inlets, outlets, and environmental sensors. In addition, an icon named Dashboard is available for displaying the PDU summary information.

The tree structure comprises three hierarchical levels.

First level	Second level	Third level
Dashboard	None	None
PDU folder*	Inlet I1	None
	Outlets folder	1 to n**
	Overcurrent Protectors folder	C1 to Cn**
	External Sensors folder	A list of connected

First level	Second level	Third level
		environmental sensors
	Feature Port folder	One of the following is displayed, depending on your configuration: • None • Asset Strip • Power CIM • LHX-20 • LHX-40
	Webcam Management folder	• Snapshots • Webcam

* The PDU folder is named "my PX" by default. The name changes after customizing the device name. See ***Naming the PDU*** (on page 98).

** n represents the final number of that component.

Note: A Webcam icon appears only when a supported Logitech® webcam is connected to the PX. See **Connecting a Logitech Webcam (Optional)** *(on page 58).*

To navigate through the tree:

1. To expand any folders, see ***Expanding the Tree*** (on page 83).
2. To show any tree item's data, click on that item. See ***Add Page Icon*** (on page 87).

Expanding the Tree

The icons representing all components implemented on or connected to the PX device are expanded by default. If they are hidden, you may expand the tree manually to show all component icons.

To expand the tree:

1. By default, the PDU folder has been expanded.

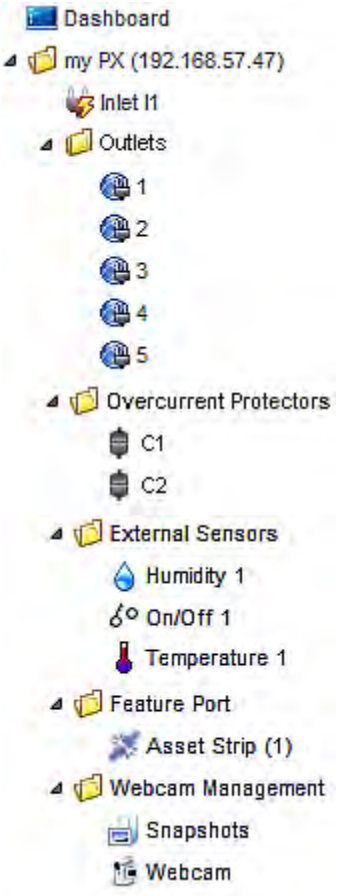
   Note: The PDU folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the PDU** *(on page 98).*

If it is not expanded, click the white arrow ▷ prior to the folder icon, or double-click the folder. The arrow then turns into a black, gradient arrow ◢, and icons of components or component groups appear below the PDU folder.

2. To expand any component group at the second level, click the white arrow ▷ prior to the folder icon, or double-click the folder.

   The arrow then turns into a black, gradient arrow ◢, and icons representing individual components appear below the group folder.

   Repeat Step 2 for other component groups you want to expand. The expanded tree looks similar to this image.



Collapsing the Tree

You can collapse the whole tree structure or a specific component group to hide all or partial tree items.

To collapse the whole tree:

- Click the black, gradient arrow ◢ prior to the PDU folder icon, or double-click the folder.

  Note: The PDU folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the PDU** *(on page 98).*

  The arrow then turns into a white arrow ▷, and all items below the PDU folder disappear.

To hide some tree items:

1. Click the black, gradient arrow ◢ prior to the component group folder that you want to collapse, or double-click the folder.

   The arrow then turns into a white arrow ▷, and all items below the folder disappear.

2. Repeat Step 1 for other component groups you want to collapse.

Adjusting the Pane

You can change the width of the pane to make the area larger or smaller.

To adjust the pane's width:

1. Move the mouse pointer to the right border of the Dominion PX Explorer pane.
2. When the mouse pointer turns into a two-way arrow, drag the border horizontally to widen or shrink the pane.

Setup Button

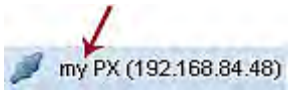
The Setup button is available for most tree items. It triggers a setup dialog where you can change settings for the selected tree item.

Status Bar

The status bar shows five pieces of information from left to right.

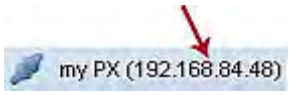
- **Device name:**

  This is the name assigned to the PX device. The default is "my PX." See ***Naming the PDU*** (on page 98).



- **IP address:**

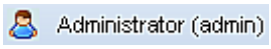
  The numbers enclosed in parentheses is the IP address assigned to the PX device. See ***Initial Network Configuration*** (on page 22) or ***Modifying the Network Settings*** (on page 101).



Tip: The presence of the device name and IP address in the status bar indicates the connection to the PX device. If the connection is lost, it shows " disconnected *" instead.*

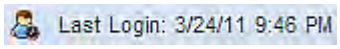
- **Login name:**

  This is the user name you used to log in to the web interface.



- **Last login time:**

  This shows the date and time this login name was used to log in to this PX device last time.



  When the mouse pointer hovers over the last login time, detailed information about the last login is displayed, including the access client and IP address.

  For the login via a local connection (serial or USB), <local> is displayed instead of an IP address.

  There are different types of access clients:

- Web GUI: Refers to the PX web interface.
- CLI: Refers to the command line interface (CLI).
  The information in parentheses following "CLI" indicates how this user was connected to the CLI.
  - *Serial*: Represents the local connection (serial or USB).
  - *SSH*: Represents the SSH connection.
  - *Telnet*: Represents the Telnet connection.

- **System date and time:**

  Current date, year, and time are displayed to the right of the bar. If positioning the mouse pointer over the system date and time, the time zone information is also displayed.

Sometimes a flag icon ( ) may appear to the far right of the bar when a communication error between the PX device and the graphical user interface (GUI) occurs. When the icon appears, you can click the icon to view the communications log. See ***Viewing the Communication Log*** (on page 249).

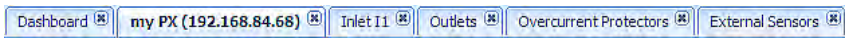
Add Page Icon

The Add Page icon , located on the top of the data pane, lets you open data pages of multiple tree items without overriding any opened page.

To open new data pages:

1. Click the Add Page icon . A new tab along with a blank data page appears.
2. Click a tree item whose data page you want to open. The data of the selected tree item is then displayed on the blank page.
3. To open more data pages, repeat Steps 1 to 2. All tabs representing opened pages are shown across the top of the page.

   The following diagram shows a multi-tab example.



4. With multiple pages opened, you can take these actions:
   - To switch to one of the opened data pages, click the corresponding tab.

     If there are too many tabs to be all shown, two arrows (and) appear at the left and right borders of the pane. Click either arrow to navigate through all tabs.

- To close any data page, click the Close button ( ) on the corresponding tab.

Logout Button

Click the logout button when you want to log out of the web interface.

Data Pane

The right pane shows the data page of the selected tree item. The data page includes the item's current status, settings and a Setup button (if available).

All tabs above the pane represent the opened data pages. The highlighted tab indicates the current selection.

You can change the width of the pane to make the area larger or smaller.

To adjust the pane's width:

1. Move the mouse pointer to the left border of the right pane.
2. When the mouse pointer turns into a two-way arrow, drag the border horizontally to widen or shrink the pane.

More Information

This section explains additional web interface elements or operations that are useful.

Warning Icon

If the value you entered in a specific field is invalid, a red warning icon appears to the right and the field in question is surrounded by a red frame as shown in this illustration.

When this occurs, position your mouse pointer over the warning icon to view the reason and modify the entered value accordingly.

The Yellow- or Red-Highlighted Reading

When a numeric sensor's reading crosses any upper or lower threshold, the background color of the whole row turns to yellow or red for alerting users.

For a discrete (on/off) sensor, the row changes the background color when the sensor enters the abnormal state.

If any circuit breaker trips, the circuit breaker's row is also highlighted in red.

See the table for the meaning of each color:

Color	State
White	The background is white in one of the following scenarios: • For a numeric sensor, no thresholds have been enabled. • If any thresholds have been enabled for a numeric sensor, the sensor reading is between the lower and upper warning thresholds. • For a discrete (on/off) sensor, the sensor state is normal. • The sensor reading or state is unavailable.
Yellow	The reading drops below the lower warning threshold or rises above the upper warning threshold.
Red	The meaning of the red color varies depending on the sensor type: • For a numeric sensor, this color indicates the reading drops below the lower critical threshold or rises above the upper critical threshold. • For a discrete (on/off) sensor, this color indicates the sensor is in the "alarmed" state. • For a circuit breaker trip sensor, it means the circuit breaker has tripped.

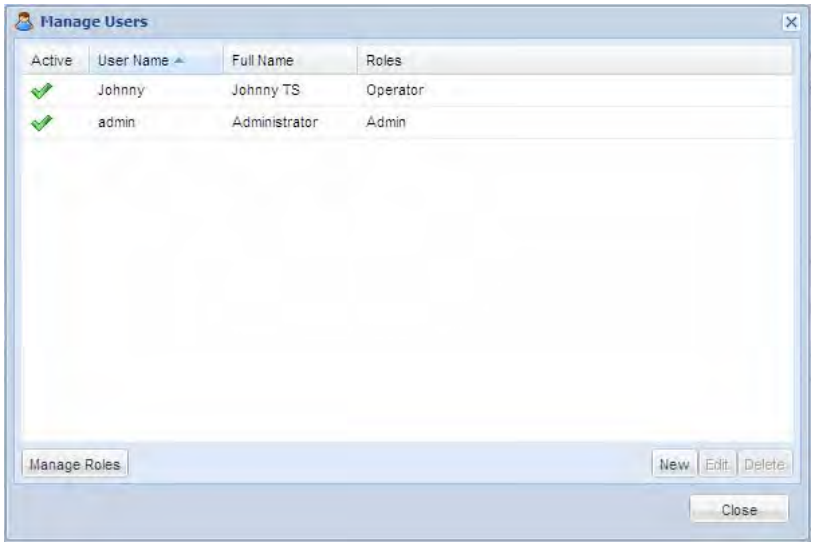
To find the exact meaning of the alert, read the information shown in the State (or Status) column:

- below lower critical: The numeric sensor's reading drops below the lower critical threshold.
- below lower warning: The numeric sensor's reading drops below the lower warning threshold.
- above upper critical: The numeric sensor's reading reaches or exceeds the upper critical threshold.
- above upper warning: The numeric sensor's reading reaches or exceeds the upper warning threshold.
- alarmed: The discrete sensor is NOT in the normal state.
- Open: The circuit breaker has tripped.

For information on the thresholds, see ***Setting Power Thresholds*** (on page 173).

Changing the View of a List

Some dialogs and data pages contain a list or table, such as the Manage Users dialog shown below. You may change the number of displayed columns or re-sort the list for better viewing the data. Note the column or sorting changes are not saved when quitting the dialog or data page. Next time when the dialog or page re-opens, the list returns to the default view.



Note: Not all dialogs support the sorting or column change functions.

Changing the Column

You can hide some columns of a list or table, or adjust a specific column's width.

To change displayed columns:

1. Hover your mouse pointer over any column header. A black triangle appears to the far right of this column header.
2. Click the black triangle, and a drop-down menu appears.
3. Point to Columns. A submenu showing all columns appears.
4. Click any column you want to deselect or select.
   - To hide a column, have its checkbox deselected.
   - To show a column, have its checkbox selected.

To change the column width:

1. Hover the mouse pointer to the right border of the desired column.
2. When the mouse pointer turns to a two-way arrow, drag the border horizontally to widen or shrink the column.

Changing the Sorting

By default, a list or table is sorted against the first column in the ascending order. You can re-sort the list in a reverse order or against a different column.

To re-sort the list by doing either of the following:

- Click the column header against which you want to sort the list.
  a. The first click sorts the list in the ascending order, indicated by a blue upward-pointing triangle .
  b. The second click reverses the sorting to the descending order, indicated by a blue downward-pointing triangle .
- Select a sorting command from the column menu.
  a. Hover your mouse pointer over the column header against which you want to sort the list. A black triangle appears to the far right of this column header.
  b. Click the black triangle, and a drop-down menu appears.
  c. Select Sort Ascending or Sort Descending.

The newly selected column header is marked with the upward- or downward-pointing triangle.

Resizing a Dialog

Most dialogs cannot be resized except for a few ones (such as the Event Log dialog), which can be resized to display more information at a time.

To resize a dialog:

1. Hover your mouse pointer over any border of the dialog.
2. When the mouse pointer turns to a double-headed arrow, drag the border vertically or horizontally to make the dialog bigger or smaller.

Browser-Defined Shortcut Menu

A shortcut menu, which is built in the web browser, may appear when right-clicking anywhere in the PX web interface.

The shortcut menu functions are defined by the browser. For example, the Back command on the Internet Explorer® (IE) shortcut menu works the same as the Back button in the IE browser. Both of these functions take you to the previous page.

For information on each shortcut menu command or item, see the online help or documentation accompanying your web browser.

Below is the illustration of the IE browser's shortcut menu. Available menu commands or items may slightly differ based on your web browser version.

Viewing the Dashboard

When you log in to the web interface, the Dashboard page is displayed by default. This page provides an overview of the PX device's status.

The page is divided into various sections according to the component type, such as inlet(s), outlets, circuit breakers and alerted sensors.

Note: If a sensor reading row is colored, it means the sensor reading already crosses one of the thresholds, or the circuit breaker has tripped. See **The Yellow- or Red-Highlighted Reading** *(on page 89).*

After clicking any other icon in the hierarchical tree, the Dashboard page is overridden. To return to the Dashboard page, click the Dashboard icon.

When the Dashboard page is opened, you can do the following to uncover or hide specific data.

To collapse any section:

1. Locate the section you want to collapse.
2. Click the upward arrow prior to the section title. The data specific to the section is hidden.

To expand a collapsed section:

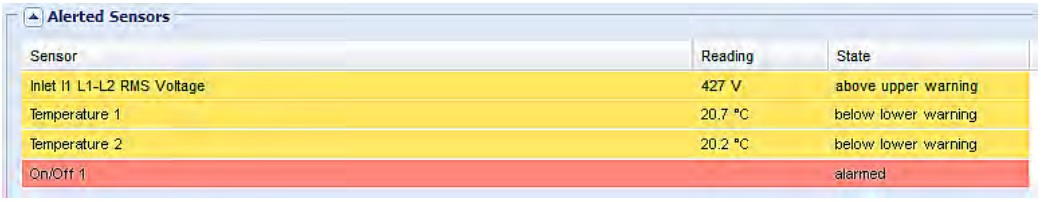
1. Locate the section you want to expand.
2. Click the downward arrow prior to the section title. The data specific to the section appears.

Alerted Sensors

One of the sections on the Dashboard page only displays critical or warning conditions detected by internal or external sensors so that you are alerted to take actions. This section is labeled Alerted Sensors.

The Alerted Sensors section lists any or all of the following:

- Any sensor that crosses the upper or lower thresholds if the thresholds are enabled
- Discrete (on/off) sensors that enter the alarmed state
- The tripped circuit breakers



For the background color meanings in this section, see ***The Yellow- or Red-Highlighted Reading*** (on page 89).

Device Management

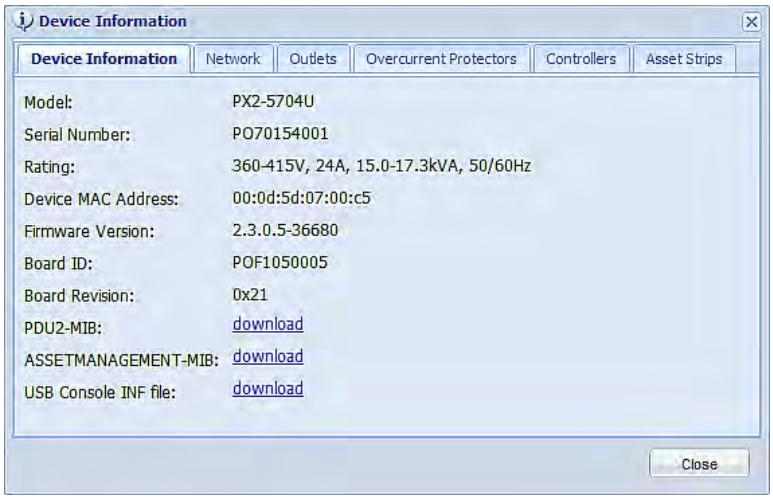
Using the web interface, you can retrieve basic hardware and software information, give the PX a new device name, set the system date and time, and modify network settings that were entered during the initial configuration process.

Displaying the PDU Information

To display information specific to the PX device that you are using, such as inlet or outlet types, trigger the Device Information dialog.

To display the PDU-specific information:

1. Choose Maintenance > Device Information. The Device Information dialog appears.



2. Click the tab containing the information you want to view. The number of available tabs varies according to the model you purchased.

Tab	Data
Device Information	General PDU information, such as model name, serial number, firmware version, hardware revision, and so on.
Network	The PDU specific network information, such as the current networking mode, IPv4 and/or IPv6 addresses and so on. This tab also indicates whether the PDU is part of an USB-cascading configuration. See

Tab	Data
	Identifying the Cascaded Devices (on page 95).
Outlets	Each outlet's receptacle type, operating voltage and rated current.
Inlets	Each inlet's plug type, rated voltage and current.
Overcurrent Protectors	Each circuit breaker's type, rated current and the outlets that it protects.
Controllers	Each inlet or outlet controller's serial number, firmware and hardware version.
Asset Strips	Each asset sensor's ID, boot version, application version and protocol version.

Note: An outlet's operating voltage is derived from the inlet's rated voltage. The result of this calculation is rounded off mathematically to the nearest integer in volt. For example, if the calculation for the minimum voltage is 380/sqrt(3)=219.39 , the web interface displays 219 V.

3. Enlarge the dialog if necessary.
4. You can re-sort the list or change the columns displayed.
5. Click Close to quit the dialog.

Tip: The firmware version is also available by clicking the PDU folder in the Dominion PX Explorer pane.

Identifying the Cascaded Devices

This section explains how to identify a cascaded PX in the Device Information dialog.

For information on how to cascade devices using USB cables, see ***Cascading the PX via USB*** (on page 29).

Note: For more information on the USB-cascading configuration, see the USB-Cascading Solution User Guide*, which is available on the* **PX2 web page** *(***http://www.raritan.com/support/dominion-px2/***) of the Raritan website.*

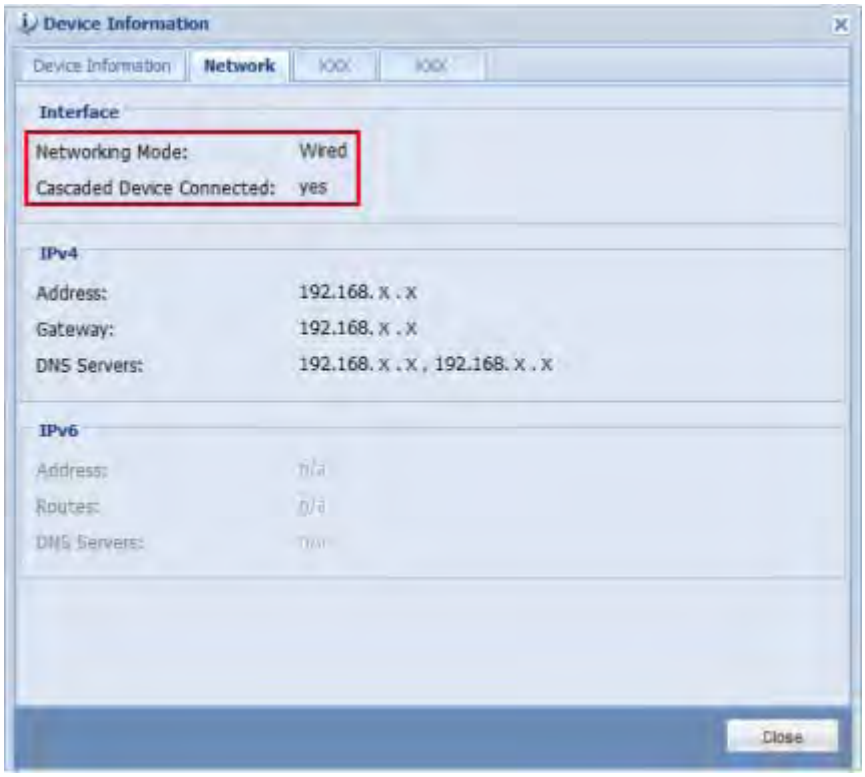
To identify the USB-cascading status of a PX device:

1. Choose Maintenance > Device Information. The Device Information dialog appears.

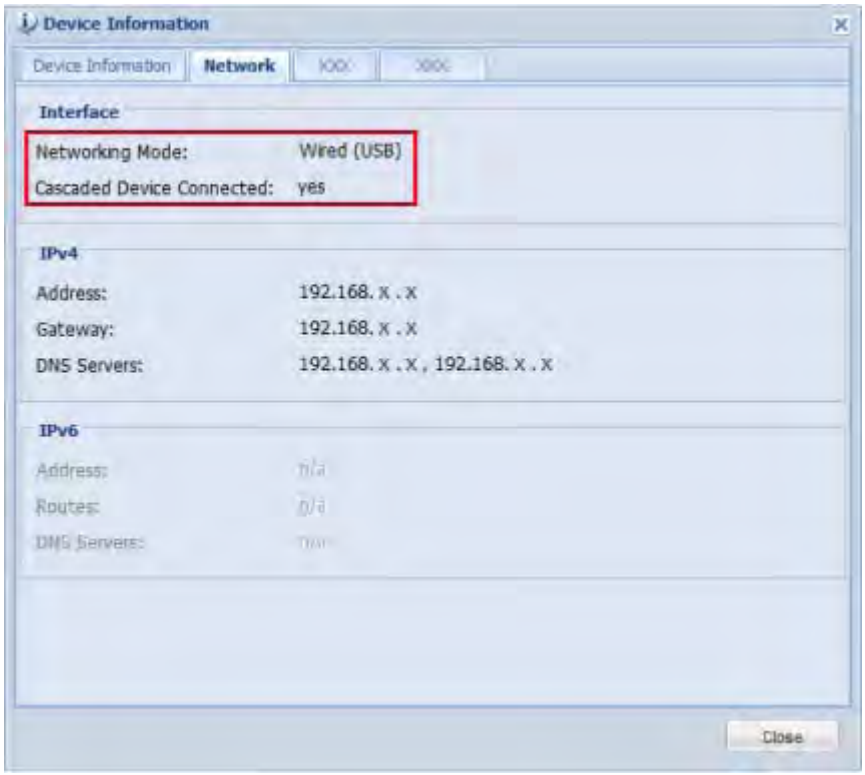
2. Select the Network tab and locate the Interface section. The Interface section contains two read-only fields: Networking Mode and Cascaded Device Connected.

Field	Description
Networking Mode	This field indicates how the PX is connected to the LAN. ▪ Wired: The device is connected to the LAN through a Category 5e/6 network cable. ▪ Wired (USB): The device is connected to the LAN through a USB-cascaded configuration. In other words, it is a slave device.
Cascaded Device Connected	This field indicates whether the PX detects the connection to a slave device on its USB-A port. ▪ yes: The connection to a slave device is detected. ▪ no: The connection to a slave device is NOT detected.

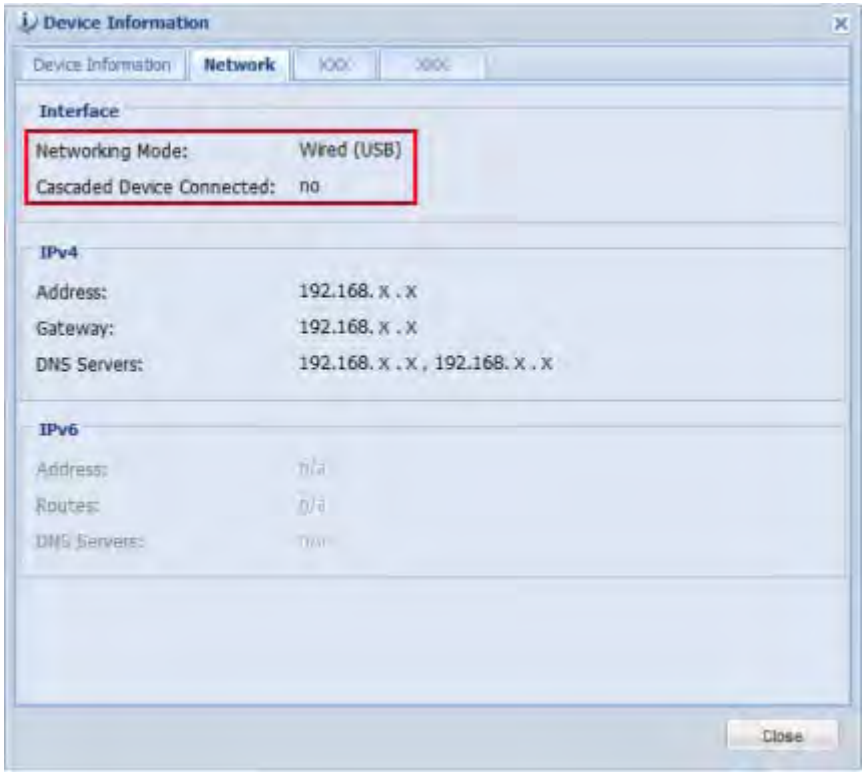
   - A master device shows *Wired* in the Networking Mode field and *yes* in the Cascaded Device Connected field.



- A slave device in the middle of the cascaded configuration shows *Wired (USB)* in the Networking Mode field and *yes* in the Cascaded Device Connected field.



- The final slave device shows *Wired (USB)* in the Networking Mode field and *no* in the Cascaded Device Connected field.



Naming the PDU

The default name for PX is *my PX*. You may give it a unique device name.

To change the device name:

1. Click the PDU folder.

   Note: The PDU folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the PDU** *(on page 98).*

2. Click Setup in the Settings section. The Pdu Setup dialog appears.
3. Type a new name in the Device Name field.
4. Click OK to save the changes.

Modifying the Network Configuration

The network settings you can change via the web interface include wired, wireless, IPv4 and/or IPv6 settings.

Modifying the Network Interface Settings

The PX supports two types of network interfaces: wired and wireless. You should configure the network interface settings according to the networking mode that applies. See ***Connecting the PX to Your Network*** (on page 20).

Wired Network Settings

The LAN interface speed and duplex mode were set during the installation and configuration process. See ***Initial Network Configuration*** (on page 22).

By default, the LAN speed and duplex mode are set to "Auto" (automatic), which works in nearly all scenarios. You can change them if there are special local requirements.

To modify the network interface settings:

1. Choose Device Settings > Network. The Network Configuration dialog appears.
2. The Interface Settings tab should have been selected. If not, click the Interface Settings tab.
3. In the Network Interface field, click the drop-down arrow, and select Wired from the list.
4. To change the LAN speed, click the drop-down arrow in the Speed field and select an option from the list.
   - Auto: System determines the optimum LAN speed through auto-negotiation.
   - 10 Mbit/s: The LAN speed is always 10 Mbps.
   - 100 Mbit/s: The LAN speed is always 100 Mbps.
5. To change the duplex mode, click the drop-down arrow in the Duplex field and select an option from the list.
   - Auto: The PX selects the optimum transmission mode through auto-negotiation.
   - Full: Data is transmitted in both directions simultaneously.
   - Half: Data is transmitted in one direction (to or from the PX device) at a time.
6. Click OK to save the changes.

Tip: You can check the LAN status in the Current State field, including the speed and duplex mode.

Wireless Network Settings

Wireless SSID, PSK and BSSID parameters were set during the installation and configuration process. See ***Initial Network Configuration*** (on page 22). You can change them via the web interface.

To modify the wireless interface settings:

1. Choose Device Settings > Network. The Network Configuration dialog appears.
2. The Interface Settings tab should have been selected. If not, click the Interface Settings tab.
3. In the Network Interface field, click the drop-down arrow, and select Wireless from the list.
4. Check the Hardware State field to ensure that the PX device has detected a wireless USB LAN adapter. If not, verify whether the USB LAN adapter is firmly connected or whether it is supported. See ***Connecting the PX to Your Network*** (on page 20).
5. Type the name of the wireless access point (AP) in the SSID field.
6. If the BSSID is available, select the Force AP BSSID checkbox, and type the MAC address in the BSSID field.

   Note: BSSID refers to the MAC address of an access point in the wireless network.

7. In the Authentication field, click the drop-down arrow, and select an appropriate option from the list.

Option	Description
No Authentication	Select this option when no authentication data is required.
PSK	A Pre-Shared Key is required for this option. ▪ In the Pre-Shared Key field, type the PSK string.

Option	Description
EAP - PEAP	PEAP stands for Protected Extensible Authentication Protocol. The following authentication data is required: ▪ Inner Authentication: Only Microsoft's Challenge Authentication Protocol Version 2 (MSCHAPv2) is supported, allowing authentication to databases that support MSCHAPv2. ▪ Identity: Type your user name for EAP authentication. ▪ Password: Type your password for EAP authentication. ▪ CA Certificate: A third-party CA certificate must be provided for EAP authentication. Click Browse to select a valid certificate file. - To view the contents of the selected certificate file, click Show. - If the selected certificate file is invalid, click Remove. Then select a new file.

8. Click OK to save the changes.

Modifying the Network Settings

The PX was configured for network connectivity during the installation and configuration process. See ***Configuring the PX*** (on page 16). If necessary, you can modify any network settings using the web interface.

Selecting the Internet Protocol

The PX device supports two types of Internet protocols -- IPv4 and IPv6. You can enable either or both Internet protocols. After enabling the desired Internet protocol(s), all but not limited to the following protocols will be compliant with the enabled Internet protocol(s):

- LDAP
- NTP
- SMTP
- SSH
- Telnet
- FTP
- SSL
- SNMP
- SysLog

To select the appropriate Internet Protocol:

1. Choose Device Settings > Network. The Network Configuration dialog appears.
2. Click the IP Protocol tab.
3. Select one checkbox according to the Internet protocol(s) you want to enable:
   - IPv4 only: Enables IPv4 only on all interfaces. This is the default.
   - IPv6 only: Enables IPv6 only on all interfaces.
   - IPv4 and IPv6: Enables both IPv4 and IPv6 on all interfaces.
4. If you selected the "IPv4 and IPv6" checkbox in the previous step, you must determine which IP address is used when the DNS resolver returns both of IPv4 and IPv6 addresses.
   - IPv4 Address: Use the IPv4 addresses returned by the DNS server.
   - IPv6 Address: Use the IPv6 addresses returned by the DNS server.
5. Click OK to save the changes.

Modifying the IPv4 Settings

You must enable the IPv4 protocol before you can modify the IPv4 network settings. See ***Selecting the Internet Protocol*** (on page 102).

To modify the IPv4 settings:

1. Choose Device Settings > Network. The Network Configuration dialog appears.

2. Click the IPv4 Settings tab.
3. In the IP Auto Configuration field, click the drop-down arrow, and select the desired option from the list.

Option	Description
DHCP	To auto-configure the PX, select DHCP. With DHCP selected, you can enter a preferred DHCP host name, which is optional. Type the host name in the Preferred Hostname field. The host name: ▪ Consists of alphanumeric characters and/or hyphens ▪ Cannot begin or end with a hyphen ▪ Cannot contain more than 63 characters ▪ Cannot contain punctuation marks, spaces, and other symbols Select the "Specify DNS server manually" checkbox if necessary. Then type the address of the primary DNS server in the Primary DNS Server field. The secondary DNS server and DNS suffix are optional.
Static	To manually assign an IP address, select Static, and enter the following information in the corresponding fields: ▪ IP address ▪ Netmask ▪ Gateway ▪ Primary DNS server ▪ Secondary DNS server (optional) ▪ DNS Suffix (optional)

4. Click OK to save the changes.

Note: The PX supports a maximum of 3 DNS servers. If two IPv4 DNS servers and two IPv6 DNS servers are available, the PX only uses the primary IPv4 and IPv6 DNS servers.

Modifying the IPv6 Settings

You must enable the IPv6 protocol before you can modify the IPv6 network settings. See ***Selecting the Internet Protocol*** (on page 102).

▶ To modify the IPv6 settings:

1. Choose Device Settings > Network. The Network Configuration dialog appears.

2. Click the IPv6 Settings tab.
3. In the IP Auto Configuration field, click the drop-down arrow, and select the desired option from the list.

Option	Description
Automatic	To auto-configure PX, select Automatic. With this option selected, you can enter a preferred host name, which is optional. Type the host name in the Preferred Hostname field. The host name: ▪ Consists of alphanumeric characters and/or hyphens ▪ Cannot begin or end with a hyphen ▪ Cannot contain more than 63 characters ▪ Cannot contain punctuation marks, spaces, and other symbols Select the "Specify DNS server manually" checkbox if necessary. Then type the address of the primary DNS server in the Primary DNS Server field. The secondary DNS server and DNS suffix are optional.
Static	To manually assign an IP address, select Static, and enter the following information in the corresponding fields: ▪ IP address ▪ Gateway ▪ Primary DNS server ▪ Secondary DNS server (optional) ▪ DNS Suffix (optional)

4. Click OK to save the changes.

Note: The PX supports a maximum of 3 DNS servers. If two IPv4 DNS servers and two IPv6 DNS servers are available, the PX only uses the primary IPv4 and IPv6 DNS servers.

Role of a DNS Server

As Internet communications are carried out on the basis of IP addresses, appropriate DNS server settings are required for mapping domain names (host names) to corresponding IP addresses, or the PX may fail to connect to the given host.

Therefore, DNS server settings are important for external authentication. With appropriate DNS settings, the PX can resolve the external authentication server's name to an IP address for establishing a connection. If the *SSL encryption* is enabled, the DNS server settings become critical since only fully qualified domain name can be used for specifying the LDAP server.

For information on external authentication, see ***Setting Up External Authentication*** (on page 147).

Modifying the Network Service Settings

The PX supports these network communication services: HTTPS, HTTP, Telnet and SSH.

HTTPS and HTTP enable the access to the web interface, and Telnet and SSH enable the access to the ***command line interface*** (see "***Using the Command Line Interface***" on page 273).

By default, SSH is enabled, Telnet is disabled, and all TCP ports for supported services are set to standard ports. You can change default settings if necessary.

Note: Telnet access is disabled by default because it communicates openly and is thus insecure.

In addition, the PX also supports the SNMP and Modbus/TCP protocols.

Changing the HTTP(S) Settings

HTTPS uses Secure Sockets Layer (SSL) technology to encrypt all traffic to and from the PX device so it is a more secure protocol than HTTP.

By default, any access to the PX device via HTTP is automatically redirected to HTTPS. See ***Forcing HTTPS Encryption*** (on page 128).

To change the HTTP or HTTPS port settings:

1. Choose Device Settings > Network Services > HTTP. The HTTP Settings dialog appears.
2. To use a different port for HTTP or HTTPS, type a new port number in the corresponding field. Valid range is 1 to 65535.

   Warning: Different network services cannot share the same TCP port.
3. Click OK to save the changes.

Changing the SSH Settings

You can enable or disable the SSH access to the command line interface, or change the default TCP port for the SSH service. In addition, you can decide to log in using either the password or the public key over the SSH connection.

To change the SSH service settings:

1. Choose Device Settings > Network Services > SSH. The SSH Settings dialog appears.
2. To use a different port, type a new port number in the field. Valid range is 1 to 65535.
3. To enable the SSH application, select the Enable SSH checkbox. To disable it, deselect the checkbox.
4. To select a different authentication method, select one of the checkboxes.
   - Allow password authentication only: Enables the password-based login only.
   - Allow public key authentication only: Enables the public key-based login only.
   - Allow password and public key authentication: Enables both the password- and public key-based login. This is the default.
5. Click OK to save the changes.

If the public key authentication is selected, you must type a valid SSH public key for each user profile to log in over the SSH connection. See ***Creating a User Profile*** (on page 120).

Changing the Telnet Settings

You can enable or disable the Telnet access to the command line interface, or change the default TCP port for the Telnet service.

To change the Telnet service settings:

1. Choose Device Settings > Network Services > Telnet. The Telnet Settings dialog appears.
2. To use a different port, type a new port number in the field. Valid range is 1 to 65535.
3. To enable the Telnet application, select the Enable Telnet Access checkbox. To disable it, deselect the checkbox.
4. Click OK to save the changes.

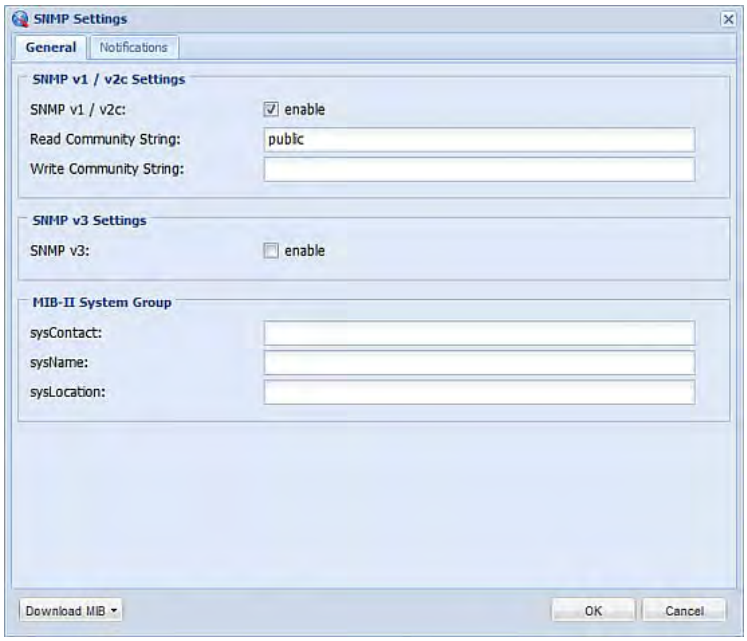
Configuring the SNMP Settings

You can enable or disable SNMP communication between an SNMP manager and the PX device. Enabling SNMP communication allows the manager to retrieve and control the power status of each outlet.

Besides, you may need to configure the SNMP destination(s) if the built-in "System SNMP Notification Rule" is enabled and the SNMP destination has not been set yet. See ***Event Rules and Actions*** (on page 180).

To configure the SNMP communication:

1. Choose Device Settings > Network Services > SNMP. The SNMP Settings dialog appears.



2. Select the "enable" checkbox in the "SNMP v1 / v2c" field to enable communication with an SNMP manager using SNMP v1 or v2c protocol.
   - Type the SNMP read-only community string in the Read Community String field. Usually the string is "public."
   - Type the read/write community string in the Write Community String field. Usually the string is "private."
3. Select the "enable" checkbox in the "SNMP v3" field to enable communication with an SNMP manager using SNMP v3 protocol.

Tip: You can permit or disallow a user to access the PX via the SNMP v3 protocol. See **Configuring Users for Encrypted SNMP v3** *(on page 264).*

4. Enter the MIB-II system group information, if applicable:
   a. sysContact - the contact person in charge of the system being contacted
   b. sysName - the name assigned to the system
   c. sysLocation - the location of the system
5. Select the MIB to be downloaded. The SNMP MIB for your PX is used by the SNMP manager.

Important: You must download the SNMP MIB for your PX to use with your SNMP manager. Click Download MIB in this dialog to download the desired MIB file. For more details, see **Downloading SNMP MIB** *(on page 270).*

6. Click OK to save the changes.

To configure SNMP notification destinations:

7. Choose Device Settings > Network Services > SNMP. The SNMP Settings dialog appears.
8. Click the Notifications tab.
9. Select the Enabled checkbox.
10. Select an SNMP notification type - SNMP v2c Trap, SNMP v2c Inform, SNMP v3 Trap, and SNMP v3 Inform.
11. Specify the SNMP notification destinations by doing the following:
    d. Specify the SNMP notification destinations in the Host field(s).
    e. Specify a port number for the destination in the Port field(s).
    f. Enter necessary information in other fields, such as the community string for SNMP Trap or authentication pass phrase for SNMP Inform. See ***Configuring SNMP Notifications*** (on page 265) for details.
12. Click OK to save the changes.

Tip: The SNMP notification destinations can be also set in the Event Rule Settings dialog. See **Modifying an Action** *(on page 214).*

Changing the Modbus/TCP Settings

You can enable or disable the Modbus/TCP access to the PX or the read-only mode, or change the default TCP port for the Modbus service.

To change the Modbus service settings:

1. Choose Device Settings > Network Services > Modbus. The Modbus Settings dialog appears.

2. To enable the Modbus access, select the Enable Modbus/TCP Access checkbox. To disable it, deselect the checkbox.
3. To use a different port, type a new port number in the field. Valid range is 1 to 65535.
4. To enable the Modbus read-only mode, select the "Enable read-only mode" checkbox. To disable it, deselect the checkbox.

Enabling Service Advertisement

The PX advertises all enabled services that are reachable using the IP network. This feature uses DNS-SD (Domain Name System-Service Discovery) and mDNS (multicast DNS). The advertised services are discovered by clients that have implemented DNS-SD and mDNS.

The advertised services include the following:

- HTTP
- HTTPS
- Telnet
- SSH
- Modbus
- json-rpc
- SNMP

This feature is enabled by default. The service advertisement feature supports both IPv4 and IPv6 protocols.

If you have set a preferred host name for IPv4 and/or IPv6, that host name can be used as the zero configuration .local host name, that is, *<preferred_host_name>.local*, where <preferred_host_name> is the preferred host name you have specified for PX. The IPv4 host name is the first priority. If an IPv4 host name is not available, then use the IPv6 host name.

Note: For information on configuring IPv4 and/or IPv6 network settings, see **Modifying the Network Settings** *(on page 101).*

To enable service advertisement:

1. Choose Device Settings > Network Services to select the Service Advertisement checkbox.
2. Click Yes on the confirmation message to switch to zero configuration advertising. The feature is enabled and the Service Advertisement checkbox is selected in the submenu.

To disable service advertisement:

1. Choose Device Settings > Network Services to deselect the Service Advertisement checkbox.

2. Click Yes on the confirmation message to switch off the zero configuration advertising. The feature is disabled and the Service Advertisement checkbox is deselected in the submenu.

Setting the Date and Time

Set the internal clock on the PX device manually, or link to a Network Time Protocol (NTP) server and let it set the date and time for the PX.

To set the date and time:

1. Choose Device Settings > Date/Time. The Configure Date/Time Settings dialog appears.
2. In the Time Zone field, click the drop-down arrow, and select your time zone from the list.
3. If the daylight saving time applies to your time zone, verify the Automatic Daylight Saving Time Adjustment checkbox is selected.

   If the daylight saving time rules are not available for the selected time zone, the checkbox is not configurable.
4. Choose one of the methods to set the date and time:
   - To customize the date and time, select the User Specified Time radio button, and then enter the date and time in appropriate fields. Use the yyyy-mm-dd format for the date and the hh:mm:ss format for the time.
     - To set the date, delete existing numbers in the Date field and type new ones, or click the calendar icon to select a date.
     - The time is measured in 24-hour format so enter 13 for 1:00pm, 14 for 2:00pm, and so on. You can enter the time by deleting existing numbers and typing new ones in the hour, minute and second fields, or clicking the arrows to adjust each number.
   - To let an NTP server set the date and time, select the "Synchronize with NTP Server" radio button. There are two ways to assign the NTP servers.

- To use the DHCP-assigned NTP servers, make sure the "Always use the servers below and ignore DHCP-provided servers" checkbox is deselected. This method is usable only when either IPv4 or IPv6 DHCP is enabled.
- To use the NTP servers that are manually specified, select the "Always use the servers below and ignore DHCP-provided servers" checkbox, and specify the primary NTP server in the First Time Server field. A secondary NTP server is optional. You may click Check NTP Servers to verify the validity and accessibility of the specified NTP servers.

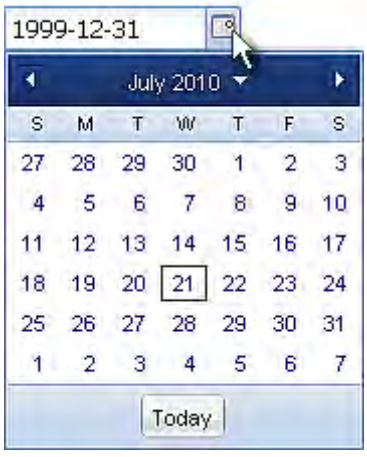
Note: If the PX device's IP address is assigned through IPv4 or IPv6 DHCP, the NTP servers can be automatically discovered. When this occurs, the data you entered in the fields of First and Second Time Server will be overridden.

5. Click OK to save the changes.

Important: If you are using Raritan's Power IQ to manage the PX, you must configure Power IQ and the PX to have the same date/time or NTP settings.

How to Use the Calendar

The calendar icon next to the Date field is a convenient tool to quickly change the year, month and date.



To select a date using the calendar:

1. To change the year shown in the calendar, do either of the following:
   - Press Ctrl+Up arrow or Ctrl+Down arrow to switch between years.

- Click , which is adjacent to the year, to show a list of years and months. Select the desired year from the list to the right and click OK. If the list does not show the desired year, click or to show additional years.

2. To change the month shown in the calendar, do one of the following:
   - Press Ctrl+Right arrow or Ctrl+Left arrow to switch between months.
   - Click or on the top of the calendar to switch between months.
   - Click , which is adjacent to the year, to show a list of years and months. Select the desired month from the list to the left and click OK.
3. To select a date, click that date on the calendar.
   - Click Today if you want to select today.

Note: On the calendar, the date for today is marked with a red frame.

Setting Up Default Measurement Units

Default measurement units are applied to the PX web and CLI interfaces across all users, including users accessing the device via external authentication servers. Default units apply only when users have not set their own preferred measurement units or the administrator has not changed preferred units for any user.

Note: To set preferred measurement units for your own, see **Setting Up Your Preferred Measurement Units** *(on page 124). If your preferences are different from the default measurement units, your preferences rather than the defaults apply to your own PX user interfaces.*

To set up default user preferences:

1. Choose User Management > Default User Preferences.

2. Update any of the following as needed:
   - In the Temperature Unit field, select °C (Celsius) or °F (Fahrenheit) as the measurement unit for temperatures.
   - In the Length Unit field, select "Meter" or "Feet" as the measurement unit for length or height.
   - In the Pressure Unit field, select "Pascal" or "psi" as the measurement unit for pressure.
3. Click OK to save the changes.

Configuring the Feature Port

The PX device supports connecting one of the following devices to its FEATURE port:

- Raritan Computer Interface Module (CIM) for KVM access. See ***Dominion KX II Configuration*** (on page 480).
- Raritan asset management sensors (asset sensors). See ***Connecting the Asset Management Sensor (Optional)*** (on page 47).
- Raritan serial access products, including Dominion KSX II or SX. See ***Dominion KSX II or SX Configuration*** (on page 484).
- Schroff® LHX-20 or LHX-40 heat exchanger. See ***Connecting a Schroff LHX Heat Exchanger (Optional)*** (on page 59).

By default, the FEATURE port can automatically detects and displays the device connected to the FEATURE port. The only exception is the Schroff® LHX-20 or LHX-40 device, which requires enabling the LHX support before the PX can detect or display it. See ***Managing the Schroff LHX Heat Exchanger*** (on page 251).

You can change the mode applied to the FEATURE port so that the PX web interface only displays the device in the manner you wish.

To configure the FEATURE port:

1. Click the Feature Port folder. The Feature Port page opens in the right pane.
2. Select the Port# 1 device on the Feature Port page, and click Setup. The Feature Port Setup dialog appears.
3. Select the desired mode in the Detected Mode field.
   - Auto: The PX automatically detects and displays the device connected to the FEATURE port. This is the default.
   - Disabled: The FEATURE port is disabled so the PX does not detect and display the connected device.

- A specific device type: The PX always displays the selected device type no matter which device is connected or whether the selected device is detected or not. Available device types are listed below.

Device type	Description
Asset Strip	Raritan asset sensors.
Power CIM	Select this type when connecting one of the following Raritan products: ▪ Raritan power CIM, D2CIM-PWR. This CIM is used to connect the PX to the Raritan digital KVM switch, Dominion KX II. ▪ Dominion KSX II ▪ Dominion SX
LHX-20	Schroff® LHX-20 heat exchanger. This device type is available only after the LHX support is enabled.
LHX-40	Schroff® LHX-40 heat exchanger. This device is available only after the LHX support is enabled.

4. Click OK to save the changes.

Configuring the Serial Port

You can change the bit-rate of the serial port labeled CONSOLE / MODEM on the PX device. The default bit-rate is 115200 bps. Bit-rate adjustment may be necessary only when you integrate the PX with another Raritan product via the serial interface. Change the bit-rate before connecting it to a Raritan product through the serial port, or there are communication problems.

Note: The serial port setting is especially useful when the PX works in conjunction with Raritan's Dominion LX KVM switch. The Dominion LX only supports 19200 bps for communications over the serial interface.

To change the serial port baud rate settings:

1. Choose Device Settings > Serial Port Settings. The Serial Port Configuration dialog appears.
2. In the Baud Rate field, click the drop-down arrow, and select the desired baud rate from the list.
3. If needed, configure GSM modem settings.
   a. Enter the SIM PIN.
   b. Select 'Use custom SMS center number' if a custom SMS will be used.
   c. Enter the SMS center number in the SMS Center field.

d. Click Advanced Information and complete all required information.

e. Enter the number of the recipient's phone in the Recipients Phone field, then click Send SMS Test to send a test SMS message.

4. Click OK.

Specifying the Device Altitude

You must specify the PX device's altitude above sea level if a Raritan differential air pressure sensor is attached. This is because the device's altitude is associated with the altitude correction factor. See ***Altitude Correction Factors*** (on page 499).

The default altitude measurement unit is meter. You can have the measurement unit vary between meter and foot according to user credentials. See ***Setting Up Your Preferred Measurement Units*** (on page 124).

To specify the altitude of the PX device:

1. Click the PDU folder.

   Note: The PDU folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the PDU** *(on page 98).*

2. Click Setup in the Settings section. The Pdu Setup dialog appears.
3. Type an integer number in the Altitude field. Depending on the measurement unit displayed, the range of valid numbers differs.
   - For meters (m), the value ranges between 0 and 3000.
   - For feet (ft), the value ranges between 0 and 9842.
4. Click OK to save the changes.

Setting Data Logging

The PX can store 120 measurements for each sensor in a memory buffer. This memory buffer is known as the data log. Sensor readings in the data log can be retrieved using SNMP.

You can configure how often measurements are written into the data log using the Measurements Per Log Entry field. Since the PX's internal sensors are measured every second, specifying a value of 60, for example, would cause measurements to be written to the data log once every minute. Since there are 120 measurements of storage per sensor, specifying a value of 60 means the log can store the last two hours of measurements before the oldest one in log gets overwritten.

Whenever measurements are written to the log, three values for each sensor are written: the average, minimum and maximum values. For example, if measurements are written every minute, the average of all measurements that occurred during the preceding 60 seconds along with the minimum and maximum measurement values are written to the log.

Note: The PX's SNMP agent must be enabled for this feature to work. See **Enabling SNMP** *(on page 263) for more details. In addition, using an NTP time server ensures accurately time-stamped measurements.*

Enabling Data Logging

By default, data logging is disabled. Only users having the "Administrator" or "Change Data Logging Settings" permissions can enable or disable this feature. See ***Setting Up Roles*** (on page 125).

To configure the data logging feature:

1. Choose Device Settings > Data Logging. The Data Logging Options dialog appears.
2. To enable the data logging feature, select the "enable" checkbox in the Enable Data Logging field.
3. Type a number in the Measurements Per Log Entry field. Valid range is from 1 to 600. The default is 60.
4. Verify that all sensor logging is enabled. If not, click Enable All in Page to have all sensors selected.
5. Click OK to save the changes.

Important: Although it is possible to selectively enable/disable logging for individual sensors on the PX in Step 4, it is NOT recommended and this capability may be removed in the future.

Configuring the SMTP Settings

The PX can be configured to send alerts or event messages to a specific administrator by email. To do this, you have to configure the SMTP settings and enter an IP address for your SMTP server and a sender's email address.

Note: See **Event Rules and Actions** *(on page 180) for information on creating event rules to send email notifications.*

To set the SMTP server settings:

1. Choose Device Settings > SMTP Server. The SMTP Server Settings dialog appears.
2. Type the name or IP address of the mail server in the Server Name field.
3. Type the port number for the SMTP server in the Port field. The default is 25.
4. Type an email address for the sender in the Sender Email Address field.
5. Type the number of email retries in the Number of Sending Retries field. The default is 2 retries.
6. Type the time interval between email retries in the "Time Interval Between Sending Retries (in minutes)" field. The time is measured in minutes. The default is 2 minutes.
7. If your SMTP server requires password authentication, do this:
   a. Select the Server Requires Authentication checkbox.
   b. Type a user name in the User Name field.
   c. Type a password in the Password field.
8. Now that you have set the SMTP settings, you can test it to ensure it works properly. Do the following:
   a. Type the recipient's email address in the Recipient Email Addresses field. Use a comma to separate multiple email addresses.
   b. Click Send Test Email.
9. Click OK to save the changes.
10. Check if the recipient(s) receives the email successfully.

Setting the EnergyWise Configuration

If a Cisco® EnergyWise energy management architecture is implemented in your place, you can enable the Cisco EnergyWise endpoint implemented on the PX device so that this device becomes part of the Cisco EnergyWise domain.

The Cisco EnergyWise feature implemented on the PX is disabled by default.

To set the Cisco EnergyWise configuration:

1. Choose Device Settings > EnergyWise. The EnergyWise Configuration dialog appears.
2. In the Enable EnergyWise field, select the "enable" checkbox to enable the Cisco EnergyWise feature.
3. In the "Domain name" field, type the name of a Cisco EnergyWise domain where the PX belongs. The domain name comprises up to 127 printable ASCII characters.
   - Spaces and asterisks are NOT acceptable.
4. In the "Domain password" field, type the authentication password (secret) for entering the Cisco EnergyWise domain. The password comprises up to 127 printable ASCII characters.
   - Spaces and asterisks are NOT acceptable.
5. In the Port field, type a User Datagram Protocol (UDP) port number for communication in the Cisco EnergyWise domain. The port ranges from 1 to 65535. Default is 43440.
6. In the "Polling interval" field, type a polling interval to determine how often the PX is queried in the Cisco EnergyWise domain. The polling interval ranges from 30 to 600 seconds. Default is 180 seconds.
7. Click OK to save the changes.

For PX2-3nnn, PX2-4nnn, and PX2-5nnn series, the parent/child relationship is formed after the Cisco EnergyWise feature is enabled.

- The PDU becomes a parent domain member.
- All outlets become children of the PDU.

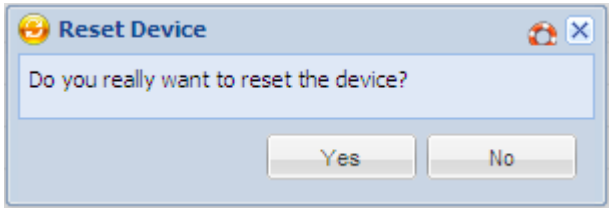
Rebooting the PX Device

You can remotely reboot the PX device via the web interface.

Resetting the PX does not interrupt the operation of connected servers because there is no loss of power to outlets. Outlets that have been powered on prior to the reset remain powered on and outlets that have been powered off prior to the reset remain powered off during and after the reset.

To reboot the device:

1. Choose Maintenance > Unit Reset. The Reset Device dialog appears.



2. Click Yes to reset the PX.
3. A message appears with a countdown timer showing the remaining time of the operation. It takes about one minute to complete.
4. When the reset is complete, the Login page opens. Now you can log back in to the PX device.

Note: If you are not redirected to the Login page after the reset is complete, click the underlined text "this link" in the message.

User Management

The PX is shipped with one built-in user profile: **admin**, which is used for initial login and configuration. This profile has full permissions, and should be reserved for the system administrator. It cannot be deleted and its permissions are not user-configurable except for the SNMP v3 permission.

All users must have a user profile, which specifies a login name and password, and contains additional (optional) information about the user. Every user profile must have at least a role to determine the user's permissions. See ***Setting Up Roles*** (on page 125).

Tip: By default, multiple users can log in simultaneously using the same login name.

Creating a User Profile

Creating new users adds a new login to the PX.

To create a user profile:

1. Choose User Management > Users. The Manage Users dialog appears.
2. Click New. The Create New User dialog appears.
3. Type the information about the user in the corresponding fields. Note that User Name, Password and Confirm Password fields are required.

Field	Type this...
User Name	The name the user enters to log in to the PX. ▪ The name can be 4 to 32 characters long. ▪ It is case sensitive. ▪ Spaces are NOT permitted
Full Name	The user's first and last names.
Password, Confirm Password	The password the user enters to log in. Type it first in the Password field and then again in the Confirm Password field. ▪ The password can be 4 to 32 characters long. ▪ It is case sensitive. ▪ Spaces are permitted.
Telephone Number	A phone number where the user can be reached.
eMail Address	An email address where the user can be reached. ▪ The email can be up to 32 characters long. ▪ It is case sensitive.

4. Select the Enabled checkbox. This is required so the user can log in to the PX device.
5. Select the "Force password change on next login" checkbox if you prefer a password change by the user when the user logs in for the first time after this checkbox is enabled.
6. Click the SNMPv3 tab to set the SNMPv3 access permission. The permission is disabled by default.
   a. To permit the SNMPv3 access by this user, select the "Enable SNMPv3 access" checkbox. Otherwise, leave the checkbox disabled.

Note: The SNMPv3 protocol must be enabled for SNMPv3 access. See **Configuring the SNMP Settings** *(on page 107).*

b. Set up SNMPv3 parameters if enabling the SNMPv3 access permission.

Field	Description
Security Level	Click the drop-down arrow to select a preferred security level from the list: ▪ NoAuthNoPriv: No authentication and no privacy. ▪ AuthNoPriv: Authentication and no privacy. ▪ AuthPriv: Authentication and privacy. This is the default.
Use Password as Authentication Pass Phrase	*This checkbox is configurable only if AuthNoPriv or AuthPriv is selected.* When the checkbox is selected, the authentication pass phrase is identical to the user's password. To specify a different authentication pass phrase, disable the checkbox.
Authentication Pass Phrase	Type the authentication pass phrase in this field if the "Use Password as Authentication Pass Phrase" checkbox is disabled. The pass phrase must consist of 8 to 32 ASCII printable characters.
Confirm Authentication Pass Phrase	Re-type the same authentication pass phrase for confirmation.
Use Authentication Pass Phrase as Privacy Pass Phrase	*This checkbox is configurable only if AuthPriv is selected.* When the checkbox is selected, the privacy pass phrase is identical to the authentication pass phrase. To specify a different privacy pass phrase, disable the checkbox.
Privacy Pass Phrase	Type the privacy pass phrase in this field if the "Use Authentication Pass Phrase as Privacy Pass Phrase" checkbox is disabled. The pass phrase must consist of 8 to 32 ASCII printable characters.
Confirm Privacy Pass Phrase	Re-type the same privacy pass phrase for confirmation.

Field	Description
Authentication Protocol	Click the drop-down arrow and select the desired authentication protocol from the list. Two protocols are available: ▪ MD5 ▪ SHA-1 (default)
Privacy Protocol	Click the drop-down arrow and select the desired privacy protocol from the list. Two protocols are available: ▪ DES (default) ▪ AES-128

7. Click the SSH tab to enter the public key if the public key authentication for the SSH service is enabled. See ***Changing the SSH Settings*** (on page 106).
   a. Open the SSH public key with a text editor.
   b. Copy and paste all contents in the text editor into the Public Key field on the SSH tab.
8. Click the Roles tab to determine the permissions of the user.
9. Select one or multiple roles by selecting corresponding checkboxes.
   - The Admin role provides full permissions.
   - The Operator role provides limited permissions for frequently-used functions. See ***Setting Up Roles*** (on page 125) for the scope of permissions. This role is selected by default.
   - If no roles meet your needs, you can:
     - *Modify the permissions of an existing role:* To modify the permissions of any role, double-click the role or highlight it and then click Edit Role. See ***Modifying a Role*** (on page 126).
     - *Create a new role by clicking the Manage Roles button:* See ***Creating a Role*** (on page 125).

   Note: With multiple roles selected, a user has the union of all roles' permissions.
10. To change any measurement units displayed in the web interface and command line interface for this new user, click the Preferences tab, and do any of the following:
    - In the Temperature Unit field, select °C (Celsius) or °F (Fahrenheit) as the measurement unit for temperatures.

- In the Length Unit field, select "Meter" or "Feet" as the measurement unit for length or height.
- In the Pressure Unit field, select "Pascal" or "psi" as the measurement unit for pressure.

A Pascal is equal to one newton per square meter. Psi stands for pounds per square inch.

Note: The measurement unit change only applies to the web interface and command line interface. Users can change the measurement units at any time by setting up their own user preferences. See **Setting Up Your Preferred Measurement Units** *(on page 124).*

Modifying a User Profile

You can change any user profile's information except for the user name.

To modify a user profile:

1. Choose User Management > Users. The Manage Users dialog appears.
2. Select the user by clicking it.
3. Click Edit or double-click the user. The Edit User 'XXX' dialog appears, where XXX is the user name.
4. Make all necessary changes to the information shown.

   To change the password, type a new password in the Password and Confirm Password fields. If the password field is left blank, the password is not changed.
5. To change the SNMPv3 access permissions, click the SNMPv3 tab and make necessary changes. For details, see Step 6 of ***Creating a User Profile*** (on page 120).
6. To change the permissions, click the Roles tab and do one of these:
   - Select or deselect any role's checkbox.
   - To modify the permissions of any role, double-click the role or highlight it and then click Edit Role. See ***Modifying a Role*** (on page 126).
7. To change the measurement unit for temperature, length or pressure, click the Preferences tab, and select a different option from the drop-down list.

   Note: The measurement unit change only applies to the web interface and command line interface.
8. Click OK to save the changes.

Deleting a User Profile

Delete outdated or redundant user profiles when necessary.

To delete user profiles:

1. Choose User Management > Users. The Manage Users dialog appears.
2. Select the user you want to delete by clicking it. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
3. Click Delete.
4. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.

Changing the User List View

You may change the number of displayed columns or re-sort the list for better viewing the data. See ***Changing the View of a List*** (on page 90).

Setting Up Your Preferred Measurement Units

The measurement units used in your PX user interfaces can be changed according to your own preferences regardless of the permissions you have.

Tip: Preferences can also be changed by administrators for specific users from the Preferences tab of the Manage Users dialog. See **Creating a User Profile** *(on page 120).*

Note: The measurement unit change only applies to the web interface and command line interface. Setting your preferences does not change the default measurement units, which apply to all users before any individual user or the administrator sets preferred measurement units on a per-user basis. See **Setting Up Default Measurement Units** *(on page 112) for information on changing default measurement units. If your preferences are different from the default measurement units, your preferences rather than the defaults apply to your own PX user interfaces.*

To change the measurement units apply to your PX graphical user interfaces:

1. Choose User Management > User Preferences. The Setup User Preferences dialog opens.
2. Update any of the following as needed:
   - In the Temperature Unit field, select °C (Celsius) or °F (Fahrenheit) as the measurement unit for temperatures.

- In the Length Unit field, select "Meter" or "Feet" as the measurement unit for length or height.
- In the Pressure Unit field, select "Pascal" or "psi" as the measurement unit for pressure.

3. Click OK to save the changes.

Setting Up Roles

A role defines the operations and functions a user is permitted to perform or access. Every user must be assigned at least a role.

The PX is shipped with two built-in roles: **Admin** and **Operator**.

- The Admin role provides full permissions. You can neither modify nor delete this role.
- The Operator role provides limited permissions for frequently-used functions. You can modify or delete this role. By default, the Operator role contains these permissions:

  - View Event Settings
  - View Local Event Log
  - Change Event Settings
  - Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration
  - Change Own Password
  - Switch Outlet (all outlets)

  Note: PX2-3nnn and PX2-4nnn series (where n is a number) are NOT outlet-switching capable so the "Switch Outlet" permission is not available.

  The Operator role is assigned to a newly created user profile by default. See ***Creating a User Profile*** (on page 120).

Creating a Role

Create a new role when you need a new combination of permissions.

To create a role:

1. Choose User Management > Roles. The Manage Roles dialog appears.

   Tip: You can also access the Manage Roles dialog by clicking the Manage Roles button in the Edit User 'XXX' dialog.

2. Click New. The Create New Role dialog appears.
3. Type the role's name in the Role Name field.
4. Type a description for the role in the Description field.

5. Click the Privileges tab to assign one or multiple permissions.
   a. Click Add. The "Add Privileges to new Role" dialog appears.
   b. Select the permission you want from the Privileges list.
   c. If the permission you selected contains any argument setting, the Arguments list is shown to the right. Then select one or multiple arguments.

      For example, if the Switch Outlet permission is selected, the Arguments list shows all outlets for you to determine which outlets this role can control. Select the desired outlets' checkboxes or select the checkbox labeled "all" if you want to select all outlets.
   d. Click Add to add the selected permission (and arguments if any).
   e. Repeat Steps *a* to *d* until you add all necessary permissions.
6. Click OK to save the changes.

Now you can assign the new role to any users. See ***Creating a User Profile*** (on page 120) or ***Modifying a User Profile*** (on page 123).

Modifying a Role

You can change an existing role's settings except for the name.

To modify a role:

1. Choose User Management > Roles. The Manage Roles dialog appears.

   Tip: You can also access the Manage Roles dialog by clicking the Manage Roles button in the Edit User 'XXX' dialog.
2. Select the role you want to modify by clicking it.
3. Click Edit or double-click the role. The Edit Role 'XXX' dialog appears, where XXX is the role name.

   Tip: You can also access the Edit Role 'XXX' dialog by clicking the Edit Role button in the Edit User 'XXX' dialog.
4. Modify the text shown in the Description field if necessary.
5. To change the permissions, click the Privileges tab.

   Note: You cannot change the Admin role's permissions.
6. To delete any permissions, do this:
   a. Select the permission you want to remove by clicking it. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
   b. Click Delete.

7. To add any permissions, do this:
   a. Click Add. The Add Privileges to Role 'XXX' dialog appears, where XXX is the role name.
   b. Select the permission you want from the Privileges list.
   c. If the permission you selected contains any argument setting, the Arguments list is shown to the right. Then select one or multiple arguments.

      For example, if the Switch Outlet permission is selected, the Arguments list shows all outlets for you to determine which outlets this role can control. Select the desired outlets' checkboxes or select the checkbox labeled "all" if you want to select all outlets.
   d. Click Add to add the selected permission (and arguments if any).
   e. Repeat Steps *a* to *d* until you add all necessary permissions.
8. To change a specific permission's arguments, do this:
   a. Select the permission by clicking it.
   b. Click Edit. The "Edit arguments of privilege 'XXX'" dialog appears, where XXX is the privilege name.

   Note: If the permission you selected does not contain any arguments, the Edit button is disabled.

   c. Select the argument you want. You can make multiple selections.
   d. Click OK.
9. Click OK to save the changes.

Deleting a Role

You can delete any role other than the Admin role.

To delete a role:

1. Choose User Management > Roles. The Manage Roles dialog appears.

   Tip: You can also access the Manage Roles dialog by clicking the Manage Roles button in the Edit User 'XXX' dialog.

2. Select the role you want to delete by clicking it. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
3. Click Delete.
4. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.

Changing the Role List View

You may change the number of displayed columns or re-sort the list for better viewing the data. See ***Changing the View of a List*** (on page 90).

Access Security Control

The PX provides tools to control access. You can require HTTPS encryption, enable the internal firewall and create firewall rules, and create login limitations.

Tip: You can also create and install the certificate or set up external authentication servers to control any access. See **Setting Up an SSL Certificate** *(on page 142) and* **Setting Up External Authentication** *(on page 147).*

Forcing HTTPS Encryption

HTTPS uses Secure Sockets Layer (SSL) technology to encrypt all traffic to and from the PX device so it is a more secure protocol than HTTP.

You can force users to access the PX web interface through the HTTPS protocol only. By default, this protocol is enabled.

To force HTTPS access to the web interface:

1. Choose Device Settings > Security > Force HTTPS for Web Access.
2. A message appears, prompting you to confirm the operation. Click Yes to enforce the HTTPS service.
3. Choose Device Settings > Security to verify the "Force HTTPS for Web Access" checkbox is selected as shown in this diagram.

If the checkbox is not selected, repeat these steps.

After enabling the HTTPS protocol, all access attempts using HTTP are redirected to HTTPS automatically.

Configuring the Firewall

The PX has a firewall that you can configure to prevent specific IP addresses and ranges of IP addresses from accessing the PX device. By default the firewall is disabled.

To configure the firewall:

1. Enable the firewall. See ***Enabling the Firewall*** (on page 129).

2. Set the default policy. See ***Changing the Default Policy*** (on page 129).
3. Create firewall rules specifying which addresses to accept and which ones to discard. See ***Creating Firewall Rules*** (on page 130).

Changes made to firewall rules take effect immediately. Any unauthorized IP activities cease instantly.

Note: The purpose of disabling the firewall by default is to prevent users from accidentally locking themselves out of the device.

Enabling the Firewall

The firewall rules, if any, take effect only after the firewall is enabled.

▶ **To enable the PX firewall:**

1. Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.
2. To enable the IPv4 firewall, click the IPv4 tab, and select the Enable IPv4 Access Control checkbox.
3. To enable the IPv6 firewall, click the IPv6 tab, and select the Enable IPv6 Access Control checkbox.
4. Click OK to save the changes.

Changing the Default Policy

After enabling the firewall, the default policy is to accept traffic from all IP addresses. This means only IP addresses discarded by a specific rule will NOT be permitted to access the PX.

You can change the default policy to Drop or Reject, in which case traffic from all IP addresses is discarded except the IP addresses accepted by a specific rule.

▶ **To change the default policy:**

1. Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.
2. To determine the default policy for IPv4 addresses:
   a. Click the IPv4 tab if necessary.
   b. Ensure the Enable IPv4 Access Control checkbox is selected.
   c. The default policy is shown in the Default Policy field. To change it, select a different policy from the drop-down list.

- Accept: Accepts traffic from all IPv4 addresses.
- Drop: Discards traffic from all IPv4 addresses, without sending any failure notification to the source host.
- Reject: Discards traffic from all IPv4 addresses, and an ICMP message is sent to the source host for failure notification.

3. To determine the default policy for IPv6 addresses:
   a. Click the IPv6 tab.
   b. Ensure the Enable IPv6 Access Control checkbox is selected.
   c. The default policy is shown in the Default Policy field. To change it, select a different policy from the drop-down list.
      - Accept: Accepts traffic from all IPv6 addresses.
      - Drop: Discards traffic from all IPv6 addresses, without sending any failure notification to the source host.
      - Reject: Discards traffic from all IPv6 addresses, and an ICMP message is sent to the source host for failure notification.
4. Click OK to save the changes. The new default policy is applied.

Creating Firewall Rules

Firewall rules determine whether to accept or discard traffic intended for the PX, based on the IP address of the host sending the traffic. When creating firewall rules, keep these principles in mind:

- **Rule order is important.**

  When traffic reaches the PX device, the rules are executed in numerical order. Only the first rule that matches the IP address determines whether the traffic is accepted or discarded. Any subsequent rules matching the IP address are ignored by the PX.

- **Subnet mask may be required.**

  When typing the IP address, you may or may not need to specify BOTH the address and a subnet mask. The default subnet mask is /32 (that is, 255.255.255.255). You must specify a subnet mask only when it is not the same as the default. For example, to specify a single address in a Class C network, use this format:

  x.x.x.x/24

  where */24* = a subnet mask of 255.255.255.0.

  To specify an entire subnet or range of addresses, change the subnet mask accordingly.

Note: Valid IP addresses range from 0.0.0.0 through 255.255.255.255. Make sure the IP addresses entered are within the scope.

To create firewall rules:

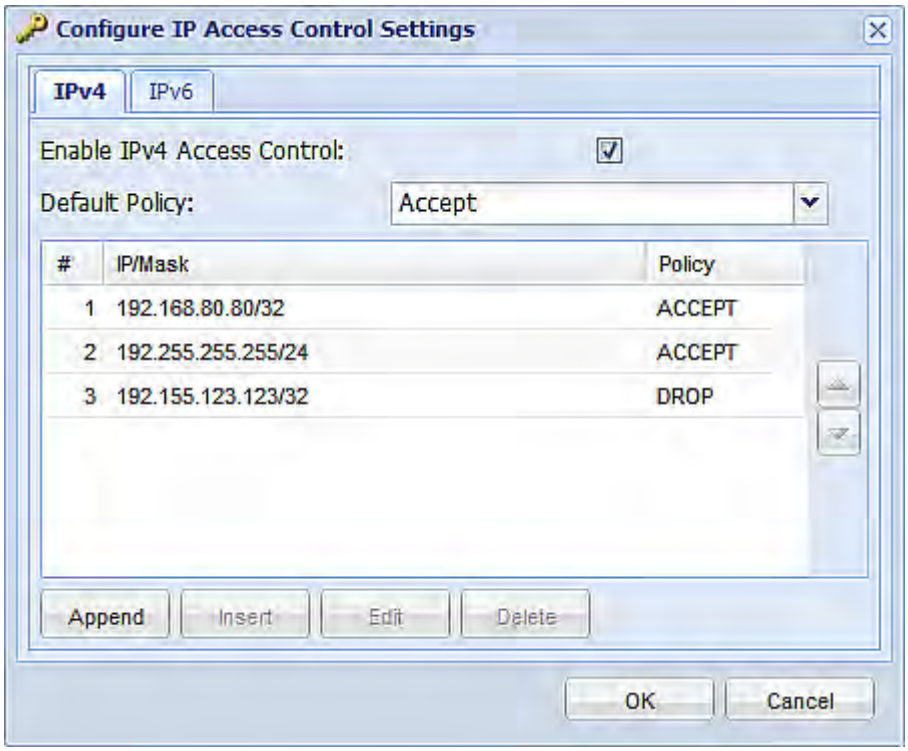
1. Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.
2. Click the IPv4 tab for creating firewall rules, or click the IPv6 tab for creating IPv6 firewall rules.
3. Ensure the Enable IPv4 Access Control checkbox is selected on the IPv4 tab, or the Enable IPv6 Access Control checkbox is selected on the IPv6 tab.
4. Create specific rules. See the table for different operations.

Action	Procedure

Add a rule to the end of the rules list	▪ Click Append. The "Append new Rule" dialog appears.
	▪ Type an IP address and subnet mask in the IP/Mask field.
	▪ Select Accept, Drop or Reject from the drop-down list in the Policy field.
	  ▪ Accept: Accepts traffic from the specified IP address(es).
	  ▪ Drop: Discards traffic from the specified IP address(es), without sending any failure notification to the source host.
	  ▪ Reject: Discards traffic from the specified IP address(es), and an ICMP message is sent to the source host for failure notification.
	▪ Click OK to save the changes.
	The system automatically numbers the rule.

Insert a rule between two existing rules	▪ Select the rule above which you want to insert a new rule. For example, to insert a rule between rules #3 and #4, select #4.
	▪ Click Insert. The "Insert new Rule" dialog appears.
	▪ Type an IP address and subnet mask in the IP/Mask field.
	▪ Select Accept, Drop or Reject from the drop-down list in the Policy field.
	  ▪ Accept: Accepts traffic from the specified IP address(es).
	  ▪ Drop: Discards traffic from the specified IP address(es), without sending any failure notification to the source host.
	  ▪ Reject: Discards traffic from the specified IP address(es), and an ICMP message is sent to the source host for failure notification.
	▪ Click OK to save the changes.
	The system inserts the rule and automatically renumbers the following rules.

5. When finished, the rules appear in the Configure IP Access Control Settings dialog.



6. Click OK to save the changes. The rules are applied.

Editing Firewall Rules

When an existing firewall rule requires updates of IP address range and/or policy, modify them accordingly.

To modify a firewall rule:

1. Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.
2. To modify the IPv4 firewall rules, click the IPv4 tab. To modify the IPv6 firewall rules, click the IPv6 tab.
3. Ensure the Enable IPv4 Access Control checkbox is selected on the IPv4 tab, or the Enable IPv6 Access Control checkbox is selected on the IPv6 tab.
4. Select the rule to be modified in the rules list.
5. Click Edit or double-click the rule. The Edit Rule dialog appears.
6. Make changes to the information shown.
7. Click OK to save the changes.

8. Click OK to quit the Configure IP Access Control Settings dialog, or the changes are lost.

Sorting Firewall Rules

The rule order determines which one of the rules matching the same IP address is performed.

To sort the firewall rules:

1. Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.
2. To sort the IPv4 firewall rules, click the IPv4 tab. To sort the IPv6 firewall rules, click the IPv6 tab.
3. Ensure the Enable IPv4 Access Control checkbox is selected on the IPv4 tab, or the Enable IPv6 Access Control checkbox is selected on the IPv6 tab.
4. Select a specific rule by clicking it.
5. Click or to move the selected rule up or down until it reaches the desired location.
6. Click OK to save the changes.

Deleting Firewall Rules

When any firewall rules become obsolete or unnecessary, remove them from the rules list.

To delete a firewall rule:

1. Choose Device Settings > Security > IP Access Control. The Configure IP Access Control Settings dialog appears.
2. To delete the IPv4 firewall rules, click the IPv4 tab. To delete the IPv6 firewall rules, click the IPv6 tab.
3. Ensure the Enable IPv4 Access Control checkbox is selected on the IPv4 tab, or the Enable IPv6 Access Control checkbox is selected on the IPv6 tab.
4. Select the rule that you want to delete. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
5. Click Delete.
6. A message appears, prompting you to confirm the operation. Click Yes to remove the selected rule(s) from the rules list.
7. Click OK to save the changes.

Setting Up User Login Controls

You can set up login controls to make it more difficult for hackers to access the PX and the devices connected to it. You can arrange to lock persons out after a specified number of failed logins, limit the number of persons who log in using the same user name at the same time, and force users to create strong passwords.

Enabling User Blocking

User blocking determines how many times a user can attempt to log in to the PX and fail authentication before the user's login is blocked.

Note that this function applies only to local authentication instead of authentication through external AA servers.

Note: If any user blocking event occurs, you can unblock that user manually by using the "unblock" CLI command via a serial connection. See **Unblocking a User** *(on page 441).*

To enable user blocking:

1. Choose Device Settings > Security > Login Settings. The Login Settings dialog appears.
2. Locate the User Blocking section.
3. To enable the user blocking feature, select the "Block user on login failure" checkbox.
4. Type a number in the "Maximum number of failed logins" field. This is the maximum number of failed logins the user is permitted before the user's login is blocked from accessing the PX device.
5. To determine how long the login is blocked, select the desired length of time from the drop-down list in the "Block timeout" field. The following describes available options.
   - Infinite: This option sets no time limit on blocking the login.
   - X min: This type of option sets the time limit to X minutes, where X is a number.
   - X h: This type of option sets the time limit to X hours, where X is a number.
   - 1 d: This option sets the time limit to 1 day.

   Tip: If the desired time option is not listed, you can manually type the desired time in this field. For example, you can type "4 min" to set the time to 4 minutes.
6. Click OK to save the changes.

Enabling Login Limitations

Login limitations determine whether more than one person can use the same login name at the same time, and how long users are permitted to stay idle before being forced to log out.

To enable login limitations:

1. Choose Device Settings > Security > Login Settings. The Login Settings dialog appears.
2. Locate the Login Limitations section.
3. To prevent more than one person from using the same login at the same time, select the "Prevent concurrent login with same username" checkbox.
4. To adjust how long users can remain idle before they are forcibly logged out by the PX, select a time option in the Idle Timeout Period field. The default is 10 minutes.
   - X min: This type of option sets the time limit to X minutes, where X is a number.
   - X h: This type of option sets the time limit to X hours, where X is a number.
   - 1 d: This option sets the time limit to 1 day.

   Tip: If the desired time option is not listed, you can manually type the desired time in this field. For example, you can type "4 min" to set the time to 4 minutes.
5. Click OK to save the changes.

Tip: Keep the idle timeout to 20 minutes or less if possible. This reduces the number of idle sessions connected, and the number of simultaneous commands sent to the PX.

Enabling Strong Passwords

Use of strong passwords makes it more difficult for intruders to crack user passwords and access the PX device. By default, strong passwords should be at least eight characters long and contain upper- and lower-case letters, numbers, and special characters, such as @ or &.

To force users to create strong passwords:

1. Choose Device Settings > Security > Password Policy. The Password Policy dialog appears.
2. Select the Strong Passwords checkbox to activate the strong password feature. The following are the default settings:

Minimum length	= 8 characters
Maximum length	= 32 characters
At least one lowercase character	= Required
At least one uppercase character	= Required
At least one numeric character	= Required
At least one special character	= Required
Number of restricted passwords in history	= 5

Note: The maximum password length accepted by the PX is 32 characters.

3. Make necessary changes to the default settings.
4. Click OK to save the changes.

Enabling Password Aging

Password Aging determines whether users are required to change passwords at regular intervals. The default interval is 60 days.

To force users to change passwords regularly:

1. Choose Device Settings > Security > Password Policy. The Password Policy dialog appears.
2. Select the Password Aging checkbox to enable the password aging feature.
3. To determine how often users are requested to change their passwords, select a number of days in the Password Aging Interval field. Users are required to change their password every time that number of days has passed.

Tip: If the desired time option is not listed, you can manually type the desired time in this field. For example, you can type "9 d" to set the password aging time to 9 days.

4. Click OK to save the changes.

Enabling and Editing the Security Banner

Use the PX restricted service agreement (security banner) if you want to require users to read and accept a security agreement when they log on to the PX.

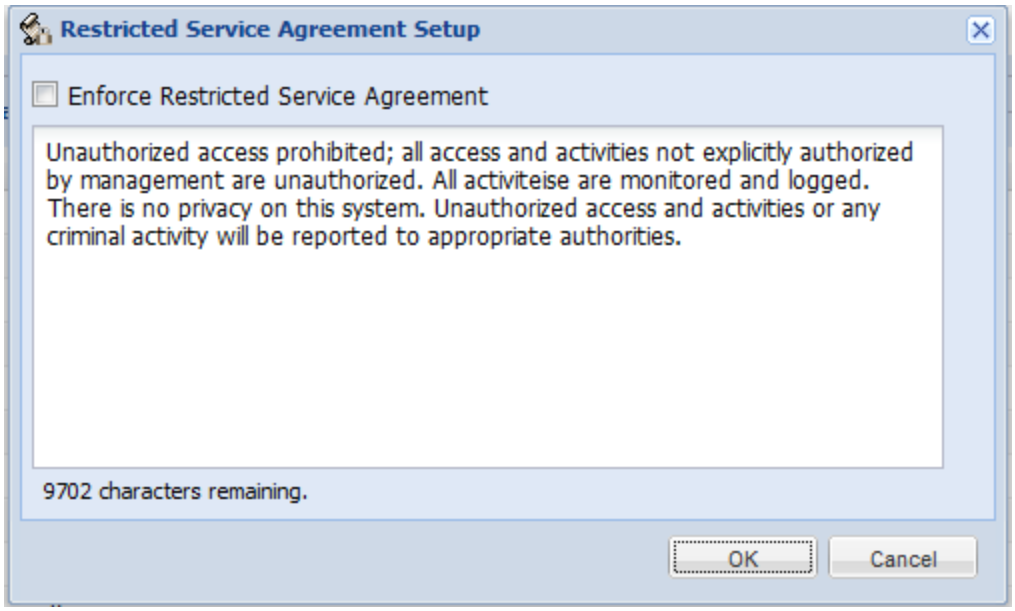
A default agreement is provided. You can edit or replace the default text as needed by typing directly in the security dialog or pasting text into it.

A maximum of 10,000 characters can be entered or pasted into the security banner.

If a user declines the agreement, they cannot log in. An event notifying you if a user has accepted or declined the agreement can be created. See ***Default Log Messages*** (on page 198).

To enable the service agreement:

1. Click Device Services > Security > Restricted Service Agreement Banner. The Restricted Service Agreement Setup dialog opens.
2. Select the Enforce Restricted Service Agreement checkbox.
3. Edit the text or replace it as needed.
4. Click OK.


Restricted Service Agreement Setup
Enforce Restricted Service Agreement
Unauthorized access prohibited; all access and activities not explicitly authorized by management are unauthorized. All activiteise are monitored and logged. There is no privacy on this system. Unauthorized access and activities or any criminal activity will be reported to appropriate authorities.
9702 characters remaining.
OK
Cancel

If the Restricted Service Agreement feature is enabled, the Restricted Service Agreement is displayed when any user logs in to the PX. Do either of the following, or you cannot successfully log in to the PX:

- In the web interface, select the checkbox labeled "I understand and accept the Restricted Service Agreement."
- In the CLI, type y when the confirmation message "I understand and accept the Restricted Service Agreement" is displayed.

Setting Up Role-Based Access Control Rules

Role-based access control rules are similar to firewall rules, except they are applied to members sharing a specific role. This enables you to grant system permissions to a specific role, based on their IP addresses.

To set up role-based access control rules:

1. Enable the feature. See ***Enabling the Feature*** (on page 138).
2. Set the default policy. See ***Changing the Default Policy*** (on page 139).
3. Create rules specifying which addresses to accept and which ones to discard when the addresses are associated with a specific role. See ***Creating Role-Based Access Control Rules*** (on page 139).

Changes made do not affect users currently logged in until the next login.

Enabling the Feature

You must enable this access control feature before any relevant rule can take effect.

To enable role-based access control rules:

1. Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
2. To enable the IPv4 firewall, click the IPv4 tab, and select the Enable Role Based Access Control for IPv4 checkbox.
3. To enable the IPv6 firewall, click the IPv6 tab, and select the Enable Role Based Access Control for IPv6 checkbox.
4. Click OK to save the changes.

Changing the Default Policy

The default policy is to accept all traffic from all IP addresses regardless of the role applied to the user.

To change the default policy:

1. Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
2. To determine the default policy for IPv4 addresses:
   a. Click the IPv4 tab if necessary.
   b. Ensure the Enable Role Based Access Control for IPv4 checkbox is selected.
   c. Select the action you want from the Default Policy drop-down list.
      - Allow: Accepts traffic from all IPv4 addresses regardless of the user's role.
      - Deny: Drops traffic from all IPv4 addresses regardless of the user's role.
3. To determine the default policy for IPv6 addresses:
   a. Click the IPv6 tab.
   b. Ensure the Enable Role Based Access Control for IPv6 checkbox is selected.
   c. Select the action you want from the Default Policy drop-down list.
      - Allow: Accepts traffic from all IPv6 addresses regardless of the user's role.
      - Deny: Drops traffic from all IPv6 addresses regardless of the user's role.
4. Click OK to save the changes.

Creating Role-Based Access Control Rules

Role-based access control rules accept or drop traffic, based on the user's role and IP address. Like firewall rules, the order of rules is important, since the rules are executed in numerical order.

To create role-based access control rules:

1. Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
2. Click the IPv4 tab for creating firewall rules, or click the IPv6 tab for creating IPv6 firewall rules.

3. Ensure the Enable Role Based Access Control for IPv4 checkbox is selected on the IPv4 tab, or the Enable Role Based Access Control for IPv6 checkbox is selected on the IPv6 tab.
4. Create specific rules:

Action	Do this...
Add a rule to the end of the rules list	▪ Click Append. The "Append new Rule" dialog appears. ▪ Type a starting IP address in the Starting IP Address field. ▪ Type an ending IP address in the Ending IP Address field. ▪ Select a role from the drop-down list in the Role field. This rule applies to members of this role only. ▪ Select Allow or Deny from the drop-down list in the Policy field. ▪ Allow: Accepts traffic from the specified IP address range when the user is a member of the specified role ▪ Deny: Drops traffic from the specified IP address range when the user is a member of the specified role ▪ Click OK to save the changes. The system automatically numbers the rule.
Insert a rule between two existing rules	▪ Select the rule above which you want to insert a new rule. For example, to insert a rule between rules #3 and #4, select #4. ▪ Click Insert. The "Insert new Rule" dialog appears. ▪ Type a starting IP address in the Starting IP Address field. ▪ Type an ending IP address in the Ending IP Address field. ▪ Select a role from the drop-down list in the Role field. This rule applies to members of this role only. ▪ Select Allow or Deny from the drop-down list in the Policy field. ▪ Allow: Accepts traffic from the specified IP address range when the user is a member of the specified role ▪ Deny: Drops traffic from the specified IP address range when the user is a member of the specified role

Action	Do this...
	▪ Click OK to save the changes. The system inserts the rule and automatically renumbers the following rules.

5. Click OK to save the changes.

Editing Role-Based Access Control Rules

You can modify existing rules when these rules do not meet your needs.

To modify a role-based access control rule:

1. Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
2. To modify the IPv4 firewall rules, click the IPv4 tab. To modify the IPv6 firewall rules, click the IPv6 tab.
3. Ensure the Enable Role Based Access Control for IPv4 checkbox is selected on the IPv4 tab, or the Enable Role Based Access Control for IPv6 checkbox is selected on the IPv6 tab.
4. Select the rule to be modified in the rules list.
5. Click Edit or double-click the rule. The Edit Rule dialog appears.
6. Make changes to the information shown.
7. Click OK to save the changes.

Sorting Role-Based Access Control Rules

Similar to firewall rules, the order of role-based access control rules determines which one of the rules matching the same IP address is performed.

To sort role-based access control rules:

1. Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
2. To sort the IPv4 firewall rules, click the IPv4 tab. To sort the IPv6 firewall rules, click the IPv6 tab.
3. Ensure the Enable Role Based Access Control for IPv4 checkbox is selected on the IPv4 tab, or the Enable Role Based Access Control for IPv6 checkbox is selected on the IPv6 tab.
4. Select a specific rule by clicking it.
5. Click or to move the selected rule up or down until it reaches the desired location.
6. Click OK to save the changes.

Deleting Role-Based Access Control Rules

When any access control rule becomes unnecessary or obsolete, remove it.

To delete a role-based access control rule:

1. Choose Device Settings > Security > Role Based Access Control. The Configure Role Based Access Control Settings dialog appears.
2. To delete the IPv4 firewall rules, click the IPv4 tab. To delete the IPv6 firewall rules, click the IPv6 tab.
3. Ensure the Enable Role Based Access Control for IPv4 checkbox is selected on the IPv4 tab, or the Enable Role Based Access Control for IPv6 checkbox is selected on the IPv6 tab.
4. Select the rule to be deleted in the rules list. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
5. Click Delete.
6. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.
7. Click OK to save the changes.

Setting Up an SSL Certificate

Having an X.509 digital certificate ensures that both parties in an SSL connection are who they say they are.

To obtain a certificate for the PX, create a Certificate Signing Request (CSR) and submit it to a certificate authority (CA). After the CA processes the information in the CSR, it provides you with an SSL certificate, which you must install on the PX device.

Note: If you are using a SSL certificate that is part of a chain of certificates, each part of the chain is signed during the validation process.

Note: See **Forcing HTTPS Encryption** *(on page 128) for instructions on forcing users to employ SSL when connecting to the PX.*

A CSR is not required in either of the following scenarios:

- You decide to generate and use a *self-signed* certificate on the PX device.
- Appropriate, valid certificate and key files are already available.

Certificate Signing Request

When appropriate certificate and key files for the PX are NOT available, one of the alternatives is to create a CSR and private key on the PX device, and send the CSR to a CA for signing the certificate.

Creating a Certificate Signing Request

Follow this procedure to create the CSR for your PX device.

To create a CSR:

1. Choose Device Settings > Security > SSL Certificate. The Manage SSL Certificate dialog appears.
2. Click the New SSL Certificate tab.
3. Provide the information requested.
   - In the Subject section:

Field	Type this information
Country (ISO Code)	The country where your company is located. Use the standard ISO country code. For a list of ISO codes, visit the ***ISO website*** (***http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm***).
State or Province	The full name of the state or province where your company is located.
Locality	The city where your company is located.
Organization	The registered name of your company.
Organizational Unit	The name of your department.
Common Name	The fully qualified domain name (FQDN) of your PX device.
Email Address	An email address where you or another administrative user can be reached.

Note: All fields in the Subject section are mandatory, except for the Organization, Organizational Unit and Email Address fields. If you generate a CSR without values entered in the required fields, you cannot obtain third party certificates.

   - In the Key Creation Parameters section:

Field	Do this
Key Length	Select the key length (bits) from the drop-down list in this field. A larger key length enhances the security, but slows down the PX device's response.
Self Sign	**For requesting a certificate signed by the CA, ensure this checkbox is NOT selected.**

Field	Do this
Challenge	Type a password. The password is used to protect the certificate or CSR. This information is optional, and the value should be 4 to 64 characters long. The password is case sensitive, so ensure you capitalize the letters correctly.
Confirm Challenge	Type the same password again for confirmation.

4. Click Create New SSL Key to create both the CSR and private key. This may take several minutes to complete.
5. To download the newly-created CSR to your computer, click Download Certificate Signing Request.
   a. You are prompted to open or save the file. Click Save to save it on your computer.
   b. After the file is stored on your computer, submit it to a CA to obtain the digital certificate.
   c. If desired, click Delete Certificate Signing Request to remove the CSR file permanently from the PX device.
6. To store the newly-created private key on your computer, click Download Key. You are prompted to open or save the file. Click Save to save it on your computer.
7. Click Close to quit the dialog.

Installing a CA-Signed Certificate

After the CA provides a signed certificate according to the CSR you submitted, you must install it on the PX device.

To install the certificate:

1. Choose Device Settings > Security > SSL Certificate. The Manage SSL Certificate dialog appears.
2. Click the New SSL Certificate tab.
3. In the Certificate File field, click Browse to select the certificate file provided by the CA.
4. Click Upload. The certificate is installed on the PX device.

Tip: To verify whether the certificate has been installed successfully, click the Active SSL Certificate tab later.

5. Click Close to quit the dialog.

Creating a Self-Signed Certificate

When appropriate certificate and key files for the PX device are unavailable, the alternative, other than submitting a CSR to the CA, is to generate a self-signed certificate.

To create and install a self-signed certificate:

1. Choose Device Settings > Security > SSL Certificate. The Manage SSL Certificate dialog appears.
2. Click the New SSL Certificate tab.
3. Provide the information requested.

Field	Type this information
Country (ISO Code)	The country where your company is located. Use the standard ISO country code. For a list of ISO codes, visit the ***ISO website*** (***http://www.iso.org/iso/country_codes/iso_3166_code_lists.htm***).
State or Province	The full name of the state or province where your company is located.
Locality	The city where your company is located.
Organization	The registered name of your company.
Organizational Unit	The name of your department.
Common Name	The fully qualified domain name (FQDN) of your PX device.
Email Address	An email address where you or another administrative user can be reached.
Key Length	Select the key length (bits) from the drop-down list in this field. A larger key length enhances the security, but slows down the PX device's response.
Self Sign	**Ensure this checkbox is selected, which indicates that you are creating a self-signed certificate.**
Validity in days	This field appears after the Self Sign checkbox is selected. Type the number of days for which the self-signed certificate is valid in this field.

Note: All fields in the Subject section are mandatory, except for the Organization, Organizational Unit and Email Address fields.

A password is not required for a self-signed certificate so the Challenge and Confirm Challenge fields disappear after the Self Sign checkbox is selected.

4. Click Create New SSL Key to create both the self-signed certificate and private key. This may take several minutes to complete.
5. You can also do any of the following:

- Click "Install Key and Certificate" to immediately install the self-signed certificate and private key. When any confirmation and security messages appear, click Yes to continue.

Tip: To verify whether the certificate has been installed successfully, click the Active SSL Certificate tab later.

- To download the self-signed certificate or private key, click Download Certificate or Download Key. You are prompted to open or save the file. Click Save to save it on your computer.
- To remove the self-signed certificate and private key permanently from the PX device, click "Delete Key and Certificate".

6. If you installed the self-signed certificate in Step 5, after the installation completes, the PX device resets and the login page re-opens.

Installing Existing Key and Certificate Files

If the SSL certificate and private key files are already available, you can install them directly without going through the process of creating a CSR or a self-signed certificate.

Note: If you are using a SSL certificate that is part of a chain of certificates, each part of the chain is signed during the validation process.

To install the existing key and certificate files:

1. Choose Device Settings > Security > SSL Certificate. The Manage SSL Certificate dialog appears.
2. Click the New SSL Certificate tab.
3. Select the "Upload Key and Certificate" checkbox. The Key File and Certificate File fields appear.
4. In the Key File field, click Browse to select the private key file.
5. In the Certificate File field, click Browse to select the certificate file.
6. Click Upload. The selected files are installed on the PX device.

Tip: To verify whether the certificate has been installed successfully, click the Active SSL Certificate tab later.

7. Click Close to quit the dialog.

Downloading Key and Certificate Files

You can download the key and certificate files currently installed on the PX device for backup or other operations. For example, you can install the files on a replacement PX device, add the certificate to your browser and so on.

To download the certificate and key files from an PX device:

1. Choose Device Settings > Security > SSL Certificate. The Manage SSL Certificate dialog appears.
2. The Active SSL Certificate tab should open. If not, click it.
3. Click Download Key to download the private key file installed on the PX device. You are prompted to open or save the file. Click Save to save it on your computer.
4. Click Download Certificate to download the certificate file installed on the PX device. You are prompted to open or save the file. Click Save to save it on your computer.
5. Click Close to quit the dialog.

Setting Up External Authentication

For security purposes, users attempting to log in to the PX must be authenticated. The PX supports the access using one of the following authentication mechanisms:

- Local database of user profiles on the PX device
- Lightweight Directory Access Protocol (LDAP)
- Remote Access Dial-In User Service (RADIUS) protocol

By default, the PX is configured for local authentication. If you stay with this method, you do not need to do anything other than create user profiles for each authorized user.

If you prefer external authentication, you must:

- Provide the PX with information about the external authentication server.
- Create user profiles for users who are authenticated externally because a user profile determines the role(s) applied to the user, and determines the permissions for the user accordingly.

When configured for LDAP authentication, all PX users must have an account on the LDAP server. Local-authentication-only users will have no access to the PX except for the admin, who always can access the PX.

Gathering the External Authentication Information

No matter which type of external authentication is preferred, the first step is to gather the data of all external authentication servers that you want to use.

Gathering the LDAP Information

It requires knowledge of your LDAP server and directory settings to configure the PX for LDAP authentication. If you are not familiar with the settings, consult your LDAP administrator for help.

To configure LDAP authentication, you need to check:

- The IP address or hostname of the LDAP server
- Whether the Secure LDAP protocol (LDAP over SSL) is being used
  - If Secure LDAP is in use, consult your LDAP administrator for the CA certificate file.
- The network port used by the LDAP server
- The type of the LDAP server, usually one of the following options:
  - *OpenLDAP*
    - If using an OpenLDAP server, consult the LDAP administrator for the Bind Distinguished Name (DN) and password.
  - *Microsoft Active Directory® (AD)*
    - If using a Microsoft Active Directory server, consult your AD administrator for the name of the Active Directory Domain.
- Bind Distinguished Name (DN) and password (if anonymous bind is NOT used)
- The Base DN of the server (used for searching for users)
- The login name attribute (or AuthorizationString)
- The user entry object class
- The user search subfilter (or BaseSearch)

Gathering the RADIUS Information

To configure RADIUS authentication, you need to collect the RADIUS information. If you are not familiar with the remote RADIUS information, consult your RADIUS administrator for help.

Below is the RADIUS information to gather:

- The IP address or host name of the RADIUS server
- Authentication protocol used by the RADIUS server
- Shared secret for a secure communication
- UDP authentication port used by the RADIUS server
- UDP accounting port used by the RADIUS server

Adding Authentication Servers

Add all external authentication servers that you want to use to the PX. Later you can use the sequence of the server list to control the authentication servers' access priority.

Adding the LDAP Server Settings

To activate and use external LDAP/LDAPS server authentication, enable LDAP authentication and enter the information you have gathered for any LDAP/LDAPS server.

Note: An LDAPS server refers to an SSL-secured LDAP server.

To add the LDAP/LDAPS server settings:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the LDAP radio button to activate remote LDAP/LDAPS server authentication.
3. Click New to add an LDAP/LDAPS server for authentication. The "Create new LDAP Server Configuration" dialog appears.
4. IP Address / Hostname - Type the IP address or hostname of your LDAP/LDAPS authentication server.

   Important: Without the SSL encryption enabled, you can type either the domain name or IP address in this field, but you must type the fully qualified domain name if the SSL encryption is enabled.

5. Type of external LDAP/LDAPS server. Choose from among the options available:
   - OpenLDAP

- Microsoft Active Directory. Active Directory is an implementation of LDAP/LDAPS directory services by Microsoft for use in Windows environments.

6. LDAP over SSL - Select this checkbox if you would like to use SSL. Secure Sockets Layer (SSL) is a cryptographic protocol that allows the PX to communicate securely with the LDAP/LDAPS server.
7. Port - The default Port is 389. Either use the standard LDAP TCP port or specify another port.
8. SSL Port - The default is 636. Either use the default port or specify another port. This field is enabled when the "LDAP over SSL" checkbox is selected.
9. Use only trusted LDAP Server Certificates - Select this checkbox if you would like to use a trusted LDAP server certificate file, that is, a certificate file signed by the CA. When NOT selected, you can use all LDAP/LDAPS server certificates, including a self-signed certificate file. A certificate file is required after enabling this option.
10. Server Certificate - Consult your authentication server administrator to get the CA certificate file for the LDAP/LDAPS server. Use the Browse button to navigate to the certificate file. This file is required when the "Use only trusted LDAP Server Certificates" checkbox is selected.

Tip: You can first upload the CA certificate file for a future use before selecting the "Use only trusted LDAP Server Certificates" checkbox, and then select the checkbox when you need to utilize the certificate file.

---

11. Anonymous Bind - For "OpenLDAP," use this checkbox to enable or disable anonymous bind.
    - To use anonymous bind, select this checkbox.
    - When a Bind DN and password are required to bind to the external LDAP/LDAPS server, deselect this checkbox.
12. Use Bind Credentials - For "Microsoft Active Directory," use this checkbox to enable or disable anonymous bind.
    - To use anonymous bind, deselect this checkbox. By default it is deselected.
    - When a Bind DN and password are required to bind to the external LDAP/LDAPS server, select this checkbox.
13. Bind DN - Specify the DN of the user who is permitted to search the LDAP directory in the defined search base. This information is required only when the Use Bind Credentials checkbox is selected.
14. Bind Password and Confirm Bind Password - Enter the Bind password in the Bind Password field first and then the Confirm Bind Password field. This information is required only when the Use Bind Credentials checkbox is selected.

15. Base DN for Search - Enter the name you want to bind against the LDAP/LDAPS (up to 31 characters), and where in the database to begin searching for the specified Base DN. An example Base Search value might be: `cn=Users,dc=raritan,dc=com`. Consult your authentication server administrator for the appropriate values to enter into these fields.
16. Type the following information in the corresponding fields. LDAP needs this information to verify user names and passwords.
    - Login name attribute (also called AuthorizationString)
    - User entry object class
    - User search subfilter (also called BaseSearch)

    Note: The PX will preoccupy the login name attribute and user entry object class with default values, which should not be changed unless required.
17. Active Directory Domain - Type the name of the Active Directory Domain. For example, testradius.com. Consult with your Active Directory Administrator for a specific domain name.
18. To verify if the authentication configuration is set correctly, you may click Test Connection to check whether the PX can connect to the remote authentication server successfully.

    Tip: You can also do this by using the Test Connection button in the Authentication Settings dialog.
19. Click OK to save the changes. The new LDAP server is listed in the Authentication Settings dialog.
20. To add additional LDAP/LDAPS servers, repeat Steps 3 to 19.
21. Click OK to save the changes. The LDAP authentication is now in place.

Note: If the PX clock and the LDAP server clock are out of sync, the certificates are considered expired and users are unable to authenticate using LDAP. To ensure proper synchronization, administrators should configure the PX and the LDAP server to use the same NTP server.

More Information about AD Configuration

For more information about the LDAP configuration using Microsoft Active Directory, see ***LDAP Configuration Illustration*** (on page 470).

Adding the RADIUS Server Settings

To activate and use external RADIUS server authentication, enable RADIUS authentication and enter the information you have gathered for any RADIUS server.

To set up RADIUS authentication:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the Radius radio button to enable remote RADIUS authentication.
3. Click New to add a RADIUS server for authentication. The "Create new RADIUS Server Configuration" dialog appears.
4. Type the IP address or host name of the RADIUS server in the IP Address / Hostname field.
5. Select an authentication protocol in the "Type of Radius Auth" field. Your choices include:
   - PAP (Password Authentication Protocol)
   - CHAP (Challenge Handshake Authentication Protocol)

   CHAP is generally considered more secure because the user name and password are encrypted, while in PAP they are transmitted in the clear.
6. By default, the PX uses the standard RADIUS port 1812 (authentication) and 1813 (accounting). If you prefer to use non-standard ports, change the ports.
7. Type the timeout period in seconds in the Timeout field. This sets the maximum amount of time to establish contact with the RADIUS server before timing out. Default is 1 second.
8. Type the number of retries permitted in the Retries field. Default is 3.
9. Type the shared secret in the Shared Secret and Confirm Shared Secret fields. The shared secret is necessary to protect communication with the RADIUS server.
10. To verify if the authentication configuration is set correctly, you may click Test Connection to check whether the PX can connect to the remote authentication server successfully.

    Tip: You can also do this by using the Test Connection button in the Authentication Settings dialog.
11. Click OK to save the changes. The new RADIUS server is listed in the Authentication Settings dialog.
12. To add additional RADIUS servers, repeat Steps 3 to 9 for each additional server.

13. Click OK to save the changes. RADIUS authentication is now in place.

Sorting the Access Order

The order of the authentication server list determines the access priority of remote authentication servers. The PX first tries to access the top server in the list for authentication, then the next one if the access to the first one fails, and so on until the PX device successfully connects to one of the listed servers.

Note: After successfully connecting to one external authentication server, the PX STOPS trying to access the remaining authentication servers in the list regardless of the user authentication result.

To re-sort the authentication server access list:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the remote authentication server whose priority you want to change.
3. Click "Move up" or "Move down" until the selected server reaches the desired position in the list.
4. Click OK to save the changes.

Testing the Server Connection

You can test the connection to any external authentication server to verify the server accessibility or the validity of the authentication settings.

To test the connection to an authentication server:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the remote authentication server that you want to test.
3. Click Test Connection to start the connection test.

Editing the Authentication Server Settings

If the configuration on any external authentication server has been changed, such as the port number, you must modify the authentication settings on the PX device accordingly, or the authentication fails.

To modify the external authentication configuration:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the remote authentication server that you want to edit.
3. Click Edit.

4. Make necessary changes to the information shown.
5. Click OK to save the changes.

Deleting the Authentication Server Settings

You can delete the authentication settings of a specific authentication server when that server is not available or not used for remote authentication.

To remove one or multiple authentication servers:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the remote authentication server that you want to remove. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
3. Click Delete.
4. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.
5. Click OK to save the changes.

Disabling External Authentication

When the remote authentication service is disabled, the PX authenticates users against the local database stored on the PX device.

To disable the external authentication service:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the Local Authentication radio button.
3. Click OK to save the changes.

Enabling External and Local Authentication Services

To make authentication function properly all the time -- even when external authentication is not available, you can enable both the local and remote authentication services.

When both authentication services are enabled, the PX follows these rules for authentication:

- When any of the remote authentication servers in the access list is accessible, the PX authenticates against the connected authentication server only.
- When the connection to every remote authentication server fails, the PX allows authentication against the local database.

To enable both authentication services:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Make sure you have selected one external authentication radio button, such as the LDAP radio button.
3. Select the "Use Local Authentication if Remote Authentication service is not available" checkbox.
4. Click OK to save the changes.

Outlet Management

PX allows you to remotely monitor and control the outlets and manage outlet settings through the web interface.

Naming Outlets

You can give each outlet a unique name up to 32 characters long to identify the equipment connected to it. The customized name is followed by the label in parentheses.

Note: In this context, the label refers to the outlet number, such as 1, 2, 3 and so on.

To name an outlet:

1. If the Outlets folder is not expanded, expand it to show all outlets. See ***Expanding the Tree*** (on page 83).
2. Click the outlet you want in the Dominion PX Explorer pane. The page specific to that outlet opens in the right pane.
3. Click Setup in the Settings section. The setup dialog for the selected outlet appears.

Tip: When the Outlets folder is selected, you can also trigger the same dialog by highlighting the outlet on the Outlets page and then clicking Setup.

4. Type a name in the Outlet Name field.
5. Click OK to save the changes.

Outlet Monitoring

The Dominion PX Explorer pane provides quick access to the outlet information. The outlet information, such as RMS current, active power, power factor, and so on, is displayed immediately after an outlet icon in the tree is selected.

Note: RMS refers to Root Mean Square, a statistical method for measuring certain types of variables. In this context, it gives the value of current that is equivalent to a DC value.

Monitoring All Outlets

You can view the current status of all outlets at a time.

To monitor all outlets:

1. If the PDU folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 83).
2. Click the Outlets folder, and the Outlets page opens in the right pane, showing all outlets with the following information:
   - Outlet number (#)
   - Outlet name
   - Outlet status (on/off)
   - Outlet sensor readings:
     - RMS current (A)
     - Active power (W)
     - Power factor
   - Non-critical outlet settings (True/False) if the PDU is outlet-switching capable

Tip: If a sensor reading row is colored, it means the sensor reading already crosses one of the thresholds, or the circuit breaker has tripped. See **The Yellow- or Red-Highlighted Reading** *(on page 89).*

Monitoring an Outlet

To view a particular outlet's detailed information, follow this procedure.

To monitor an outlet:

1. If the Outlets folder is not expanded, expand it to show all outlets. See ***Expanding the Tree*** (on page 83).
2. Click the outlet you want in the Dominion PX Explorer pane, and the outlet's details are shown in the right pane, including:
   - Outlet label (number)
   - Outlet name
   - Outlet status (on/off)

   Note: The outlet status is only available on a outlet-switching capable PX device.

   - Line pair associated with this outlet
   - Overcurrent protector that protects this outlet, such as a circuit breaker
   - Outlet state on device startup
   - Power off period during power cycle
   - Non-critical outlet settings (False/True)

   Note: The above three pieces of information is only available on a outlet-switching capable PX device.

   - Outlet sensor readings:
     - RMS current (A)
     - RMS voltage (V)
     - Active power (W)
     - Apparent power (VA)
     - Power factor
     - Active energy (Wh)

   The outlet readings turn to zero if the associated circuit breaker trips or the fuse blows.

Note: If your PX device is not implemented with any overcurrent protectors, the overcurrent protector information is not available.

Note: If a sensor reading row is colored, it means the sensor reading already crosses one of the thresholds, or the circuit breaker has tripped. See **The Yellow- or Red-Highlighted Reading** *(on page 89).*

Outlet Switching

This section only applies to outlet-switching capable PDUs.

You can change the power status of one or multiple outlets with one click in the web interface. To change the power state, the PDU must be implemented with the outlet switching function, and you must have the *Switch Outlet* permission.

Note: If your PX device does not support outlet switching, no outlets can be switched on/off regardless of the permissions you have.

Switching Multiple or All Outlets

This section only applies to outlet-switching capable PDUs.

The power state can be changed regardless of each outlet's current state. That is, you can turn the outlets on or off or power cycle them even if they are already in the selected state.

Power cycling the outlet(s) turns the outlet(s) off and then back on.

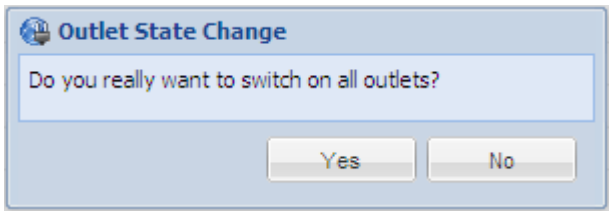
To turn on or off multiple or all outlets, or cycle their power:

1. If the PDU folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 83).

   Note: The PDU folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the PDU** *(on page 98).*

2. Click the Outlets folder, and the Outlets page opens in the right pane.
3. Select the outlets whose power states you want to change, and ensure their checkboxes are all selected.
   - To select all outlets, select the top checkbox in the header row.
   - To select multiple outlets, select the checkbox of each desired outlet one by one.
   - To select a single outlet, select that outlet's checkbox.
4. Click On, Off, or Cycle.

5. A dialog for confirming the operation appears. Click Yes and all outlets switch ON, OFF, or cycle their power.



Switching an Outlet

This section only applies to outlet-switching capable PDUs.

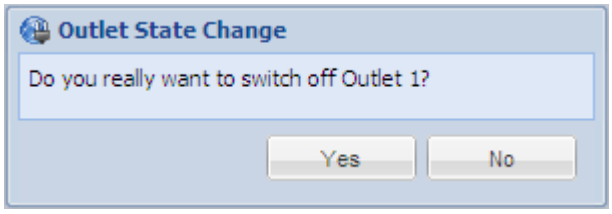
You can turn on or off or power cycle any outlet regardless of the outlet's current state.

Power cycling the outlet(s) turns the outlet(s) off and then back on.

There are different ways to turn an outlet on or off, or cycle its power.

To control an outlet with a particular outlet icon selected:

1. If the Outlets folder is not expanded, expand it to show all outlets. See ***Expanding the Tree*** (on page 83).
2. Click the outlet you want in the PX Explorer pane, and locate the Control section in the right pane.
3. Click On, Off, or Cycle.
4. A dialog for confirming the operation appears. Click Yes and the outlet switches ON, OFF, or cycles its power.



To control an outlet with the Outlets folder icon selected:

1. If the PDU folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 83).

   Note: The PDU folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the PDU** *(on page 98).*

2. Click the Outlets folder, and the Outlets page opens in the right pane.

3. Click the outlet you want in the right pane, and the corresponding checkbox is selected.
4. Click On, Off, or Cycle.
5. A dialog for confirming the operation appears. Click Yes and the outlet switches ON, OFF, or cycles its power.

Setting the Default Outlet State

This section only applies to outlet-switching capable PDUs.

Default outlet state determines the initial power state of outlets after the PX device powers up. You can set up the default outlet state for all outlets or for a specific outlet. Note that the value set for an individual outlet always overrides the value set for all outlets.

When removing power from the PDU, you must keep it unpowered for a minimum of 10 seconds. Otherwise, the default outlet state settings may not work properly after powering up the PDU again.

Setting the PDU-Defined Default State

This section only applies to outlet-switching capable PDUs.

This procedure sets the PDU-defined outlet state, which determines the initial power state of all outlets after powering up the PX device.

Tip: To set a different state on a particular outlet, see **Setting the Outlet-Specific Default State** *(on page 161).*

To set the default state for all outlets:

1. Click the PDU folder.

   Note: The PDU folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the PDU** *(on page 98).*

2. Click Setup in the Settings section. The Pdu Setup dialog appears.
3. In the "Outlet state on device startup" field, click the drop-down arrow and select an option from the list.
   - on: Turns on all outlets when the PX device powers up.
   - off: Turns off all outlets when the PX device powers up.
   - last known: Restores all outlets to their previous power states before the PX device was powered off.
4. Click OK to save the changes.

Setting the Outlet-Specific Default State

This section only applies to outlet-switching capable PDUs.

By default, the power state of each outlet follows the PDU-defined setting. Setting the default state of a particular outlet to a value other than "PDU defined" overrides the PDU-defined setting on that outlet.

To set the default power state for a specific outlet:

1. If the Outlets folder is not expanded, expand it to show all outlets. See ***Expanding the Tree*** (on page 83).
2. Click the outlet you want in the Dominion PX Explorer pane. The page specific to that outlet opens in the right pane.
3. Click Setup in the Settings section. The setup dialog for the selected outlet appears.

   Tip: When the Outlets folder is selected, you can also trigger the same dialog by highlighting the outlet on the Outlets page and then clicking Setup.

4. In the "State on device startup" field, click the drop-down arrow and select an option from the list.
   - on: Turns on this outlet when the PX device powers up.
   - off: Turns off this outlet when the PX device powers up.
   - last known: Restores this outlet to the previous power state before the PX device was powered off.
   - PDU defined: The outlet's default power state is determined by the PDU-defined state. See ***Setting the PDU-Defined Default State*** (on page 160)

   Tip: The information in parentheses following the option "PDU defined" indicates the current PDU-defined selection.

5. Click OK to save the changes.

Changing the Cycling Power-Off Period

This section only applies to outlet-switching capable PDUs.

Power cycling the outlet(s) turns the outlet(s) off and then back on. You can adjust the length of the time it takes for the outlets to turn back on after they are switched OFF during the power cycle.

The power-off period of power cycle can be set for all outlets or for an individual outlet. Note that the value set for an individual outlet always overrides the value set for all outlets.

Changing the PDU-Defined Cycling Power-Off Period

This section only applies to outlet-switching capable PDUs.

The "PDU-defined" power-off period determines how long it takes for all outlets to turn on after they are turned OFF during the power cycle. The default PDU-defined power-off period is 10 seconds (10 s).

Note: To set a different power-off period on a particular outlet, see **Changing the Outlet-Specific Cycling Power-Off Period** *(on page 163).*

To set the power-off period for all outlets:

1. Click the PDU folder.

   Note: The PDU folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the PDU** *(on page 98).*

2. Click Setup in the Settings section. The Pdu Setup dialog appears.
3. In the "Power off period during power cycle" field, click the drop-down arrow and select an option from the list. Valid range is zero second to one hour.

   Time units in the list are explained below:

   - s: second(s)
   - min: minute(s)
   - h: hour(s)

   You can also type a value if the desired time is not listed. For example, type "15 s" if you want a 15-second delay.
4. Click OK to save the changes.

Tip: When there are a large number of outlets, set the value to a lower number so that you can avoid a long wait before all the outlets are available again.

Changing the Outlet-Specific Cycling Power-Off Period

This section only applies to outlet-switching capable PDUs.

When the power cycling occurs, the default power-off period of each outlet follows the PDU-defined setting. You can adjust the power-off period of a particular outlet so that it is turned back on after a different power-off period.

Setting the power-off period for a particular outlet to a value other than "PDU defined" overrides the PDU-defined setting on that outlet.

To set the power-off period for a specific outlet:

1. If the Outlets folder is not expanded, expand it to show all outlets. See ***Expanding the Tree*** (on page 83).
2. Click the outlet you want in the Dominion PX Explorer pane. The page specific to that outlet opens in the right pane.
3. Click Setup in the Settings section. The setup dialog for the selected outlet appears.

   Tip: When the Outlets folder is selected, you can also trigger the same dialog by highlighting the outlet on the Outlets page and then clicking Setup.

4. In the "Power off period during power cycle" field, click the drop-down arrow and select an option from the list. Valid range is zero second to one hour.

   Time units in the list are explained below:

   - s: second(s)
   - min: minute(s)
   - h: hour(s)
   - To make the outlet's power-off period identical to the PDU-defined setting, select the "PDU defined" option. See ***Changing the PDU-Defined Cycling Power-Off Period*** (on page 162).

   Tip: The information in parentheses following the option "PDU defined" indicates the current PDU-defined selection.

   You can also type a value if the desired time is not listed. For example, type "15 s" if you want a 15-second delay.

5. Click OK to save the changes.

Setting the Initialization Delay

This section only applies to outlet-switching capable PDUs.

The outlet initialization delay determines how long the PX device waits before providing power to all outlets during power cycling or after recovering from a temporary power loss. This is useful in cases where power may not initially be stable after being restored, or when UPS batteries may be charging.

To set the initialization delay for all outlets:

1. Click the PDU folder.

   Note: The PDU folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the PDU** *(on page 98).*

2. Click Setup in the Settings section. The Pdu Setup dialog appears.
3. In the "Outlet initialization delay on device startup" field, click the drop-down arrow and select an option from the list. Valid range is 1 second to 1 hour.

   Time units in the list are explained below:

   - s: second(s)
   - min: minute(s)
   - h: hour(s)

4. Click OK to save the changes.

Tip: When there are a large number of outlets, set the value to a lower number so that you can avoid a long wait before all the outlets are available again.

Setting the Inrush Guard Delay

This section only applies to outlet-switching capable PDUs.

When electrical devices are turned on, they can initially draw a very large current known as inrush current. Inrush current typically lasts for 20-40 milliseconds. The inrush guard delay feature prevents a circuit breaker trip due to the combined inrush current of many devices turned on at the same time. For example, if the inrush guard delay is set to 100 milliseconds and two or more outlets are turned on at the same time, the PDU will sequentially turn the outlets on with a 100 millisecond delay occurring between each one.

To set the inrush guard delay time:

1. Click the PDU folder.

   Note: The PDU folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the PDU** *(on page 98).*

2. Click Setup in the Settings section. The Pdu Setup dialog appears.
3. In the Inrush Guard Delay field, click the drop-down arrow and select an option from the list. Valid range is from 100 milliseconds to 100 seconds.

   Time units in the list are explained below:

   - ms: millisecond(s)
   - s: second(s)

4. Click OK to save the changes.

Setting the Outlet Power-On Sequence

This section only applies to outlet-switching capable PDUs.

By default, the outlets are sequentially powered on in ascending order from outlet 1 to the highest-numbered outlet when turning ON or power cycling all outlets on the PX device. You can change the order in which the outlets power ON. This is useful when there is a specific order in which the connected IT equipment should be powered up.

To set the outlet power-on sequence:

1. Trigger the Outlet Sequence Setup dialog by doing either of the following:

   - Click the Outlets folder, and the Outlets page opens in the right pane. Click Sequence Setup.

- Click the PDU folder, and then the Setup button in the Outlet Sequence section.

Note: The PDU folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the PDU** *(on page 98).*

The Outlet Sequence Setup dialog appears, with the current power-up sequence indicated by the outlet order in the list.

2. To change the priority of an outlet, select it from the list and click one of the following buttons.
   - : Moves the outlet to the top of the list, making it the first outlet to receive power.
   - : Moves the outlet up one position in the list.
   - : Moves the outlet down one position in the list.
   - : Moves the outlet to the bottom of the list, making it the final outlet to receive power.
   - : Restores the list to the default power-up sequence, that is, the ascending order.
3. You can re-sort the list or change the columns displayed. Note that re-sorting the list makes changes to the outlet power-up sequence.
4. Click OK to save the changes.

Next time when power cycling the PDU, it will turn on all outlets based on the new order of the list.

Setting the Outlet-Specific Power-On Delay

This section only applies to outlet-switching capable PDUs.

You can make a power-on delay occur between two outlets that are turned on consecutively when the PDU turns on all outlets.

For example, if the power-up sequence is Outlet 1 through Outlet 12, and you want the PDU to wait for 5 seconds after turning on Outlet 3 before turning on Outlet 4, assign a delay of 5 seconds on Outlet 3.

To set the outlet-specific power-on delay:

1. Trigger the Outlet Sequence Setup dialog by doing either of the following:
   - Click the Outlets folder, and the Outlets page opens in the right pane. Click Sequence Setup.

- Click the PDU folder, and then the Setup button in the Outlet Sequence section.

2. Click the Delay column of the outlet where a delay is intended after this outlet is turned on, delete the existing value and type a new number in seconds. The number can be a decimal number.
   - To disable the delay, simply type the number 0 (zero).
3. Repeat the above step to change the delay settings of additional outlets.
4. Click OK to save the changes.

Setting Non-Critical Outlets and Load Shedding Mode

This section only applies to outlet-switching capable PDUs.

When a UPS supplying power to the PDU switches into battery backup operation, it may be desirable to switch off non-critical outlets to conserve UPS battery life. This feature is known as load shedding.

Activation of load shedding can be accomplished using the web interface, SNMP or CLI, or triggered by the contact closure sensors.

Outlets that are turned off when load shedding is activated are called non-critical. Outlets that are not affected by load shedding are called critical outlets. When load shedding is deactivated, the PDU will turn back on all non-critical outlets. By default, all outlets are configured as critical until you configure them otherwise.

Marking All Outlets

This section only applies to outlet-switching capable PDUs.

You can configure all critical and non-critical outlets at a time.

To mark all outlets at a time:

1. Click the PDU folder.

   Note: The PDU folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the PDU** *(on page 98).*

2. Click Setup Non-Critical Outlets in the Load Shedding section. The "Non-critical Outlet Setup" dialog appears.

   Tip: This dialog can be also triggered by clicking the "Non-critical Outlet Setup" button on the Outlets page when selecting the Outlets folder.

3. To mark an outlet as "non-critical," select it from the "Critical outlets" list box, and click to move it to the "Non-critical outlets" list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

   To move all outlets in the "Critical outlets" list box to the "Non-critical outlets" list box at a time, click .

4. To mark an outlet as "critical," select it from the "Non-critical outlets" list box, and click to move it to the "Critical outlets" list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

   To move all outlets in the "Non-critical outlets" list box to the "Critical outlets" list box at a time, click .

5. Click OK to save the changes.

Marking an Outlet

This section only applies to outlet-switching capable PDUs.

You can also choose to mark a specific outlet as a critical or non-critical outlet in its setup dialog.

To mark an outlet:

1. If the Outlets folder is not expanded, expand it to show all outlets. See ***Expanding the Tree*** (on page 83).
2. Click the outlet you want in the Dominion PX Explorer pane. The page specific to that outlet opens in the right pane.
3. Click Setup in the Settings section. The setup dialog for the selected outlet appears.

   Tip: When the Outlets folder is selected, you can also trigger the same dialog by highlighting the outlet on the Outlets page and then clicking Setup.

4. In the Non Critical field, select an option from the drop-down list.
   - True: This option marks the outlet as a non-critical outlet.
   - False: This option marks the outlet as a critical outlet.
5. Click OK to save the changes.

Activating or Deactivating the Load Shedding Mode

This section only applies to outlet-switching capable PDUs.

When entering the load shedding mode, PX turns OFF all non-critical outlets.

When exiting from the load shedding mode, PX turns ON all non-critical outlets that were ON before entering the load shedding mode.

You can activate or deactivate this mode from the PDU or Outlets page.

To enter or exit from the load shedding mode from the PDU page:

1. Click the PDU folder.

   Note: The PDU folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the PDU** *(on page 98).*

2. In the Load Shedding section, click Enable Load Shedding to enter the load shedding mode or Disable Load Shedding to deactivate the mode.
3. You are then prompted to confirm this operation.
4. If you chose to activate the mode in the previous step, click Yes to turn off all non-critical outlets. If you chose to deactivate the mode, click Yes to turn on all non-critical outlets that were previously ON prior to the load shedding mode.

To enter or exit from the load shedding mode from the Outlets page:

1. If the PDU folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 83).
2. Click the Outlets folder, and the Outlets page opens in the right pane.
3. To enter the load shedding mode, select the Load Shedding checkbox. To exit from the load shedding mode, deselect the Load Shedding checkbox.
4. You are then prompted to confirm this operation.
5. If you chose to activate the mode in the previous step, click Yes to turn off all non-critical outlets. If you chose to deactivate the mode, click Yes to turn on all non-critical outlets that were previously ON prior to the load shedding mode.

Note: During the load shedding mode, this icon appears on all non-critical outlets on the Outlets page, and you CANNOT turn on any of them.

Inlet and Circuit Breaker Management

You can name each inlet and circuit breaker or monitor their status.

Naming the Inlet

You can customize the inlet's name for your own purpose. The customized name is followed by the label in parentheses.

Note: In this context, the label refers to the inlet number, such as I1.

To name the inlet:

1. If the PDU folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 83).

   Note: The PDU folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the PDU** *(on page 98).*

2. Click Inlet I1 in the Dominion PX Explorer pane, and the Inlet I1 page opens in the right pane.
3. Click Setup. The Inlet I1 Setup dialog appears.
4. Type a new name in the Name field.
5. Click OK to save the changes.

Naming Circuit Breakers

You can name each circuit breaker for easily identifying them.

The customized name is followed by the label in parentheses.

Note: In this context, the label refers to the circuit breaker number, such as C1.

To name a circuit breaker:

1. Expand the Overcurrent Protectors folder to show all circuit breakers in the Dominion PX Explorer pane. See ***Expanding the Tree*** (on page 83).
2. Click the desired circuit breaker in the Dominion PX Explorer pane, and the page for this circuit breaker opens in the right pane.
3. Click Setup. The Overcurrent Protector Setup dialog appears.

Tip: This dialog can be also triggered by clicking Setup on the Overcurrent Protectors page when the Overcurrent Protectors folder is selected in the Dominion PX Explorer pane.

4. Type a new name in the Name field.
5. Click OK to save the changes.

Monitoring the Inlet

You can view the inlet's details, including its:

- Label (number)
- Customized name
- Inlet sensor readings:
  - RMS current per line (A)
  - RMS voltage per line pair (V)
  - Active power (W)
  - Apparent power (VA)
  - Power factor
  - Active energy (Wh)
  - Unbalanced load percentage

Note: If a sensor reading row is colored, it means the sensor reading already crosses one of the thresholds. See **The Yellow- or Red-Highlighted Reading** *(on page 89).*

There are two ways to access the inlet information.

To get the overview of the inlet status:

1. Click the Dashboard icon in the Dominion PX Explorer pane, and the Dashboard page opens in the right pane.
2. Locate the Inlet section on the Dashboard page.

To view the inlet's details:

1. If the PDU folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 83).

   Note: The PDU folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the PDU** *(on page 98).*

2. Click Inlet I1 in the Dominion PX Explorer pane, and the Inlet I1 page opens in the right pane.

Monitoring Circuit Breakers

Each circuit breaker on the PX device delivers power to a bank of outlets, and draws power from one or two lines.

You can view the circuit breaker's details, including its:

- Label (number)
- Name
- Status (closed/open)
- Its type
- Lines associated with this circuit breaker
- Outlets protected by this circuit breaker
- Sensor readings:

  - Current drawn (A)

  - Current remaining (A)

Note: If a sensor reading row is colored, it means the sensor reading already crosses one of the thresholds, or the circuit breaker has tripped. See **The Yellow- or Red-Highlighted Reading** *(on page 89).*

You can view the summary of all circuit breakers at a time or the status of individual circuit breakers.

To view all circuit breakers' status:

You can check the status of all circuit breakers at a time via either the Dashboard or Overcurrent Protectors page.

- **Using the Dashboard page:**

a. Click the Dashboard icon in the Dominion PX Explorer pane, and the Dashboard page opens in the right pane.

b. Locate the Overcurrent Protectors section on the Dashboard page.

- **Using the Overcurrent Protectors page:**

a. If the PDU folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 83).

b. Click Overcurrent Protectors in the Dominion PX Explorer pane, and the Overcurrent Protectors page opens in the right pane.

To view a circuit breaker's details:

1. Expand the Overcurrent Protectors folder to show all circuit breakers in the Dominion PX Explorer pane. See ***Expanding the Tree*** (on page 83).
2. Click the desired circuit breaker in the Dominion PX Explorer pane, and the page for this circuit breaker opens in the right pane.

Setting Power Thresholds

Setting and enabling the thresholds causes the PX to generate alert notifications when it detects that any component's power state crosses the thresholds.

There are four thresholds for each sensor: Lower Critical, Lower Warning, Upper Warning and Upper Critical.

- Upper and Lower Warning thresholds indicate the sensor reading enters the warning range before the critical threshold.
- Upper and Lower Critical thresholds indicate the sensor reading is at the critical level.

To avoid generating a large amount of alert events, the deassertion hysteresis for each threshold is enabled. You can change the default hysteresis value if necessary. For more information on the deassertion hysteresis, see ***What is Deassertion Hysteresis?*** (on page 178).

Note: After setting the thresholds, remember to configure the event rules. See **Event Rules and Actions** *(on page 180).*

Setting an Outlet's Thresholds

You can set up the thresholds, deassertion hysteresis and assertion timeout for a particular outlet.

The threshold values set for an individual outlet will override the bulk threshold values stored on that outlet.

To set the thresholds for an outlet:

1. If the Outlets folder is not expanded, expand it to show all outlets. See ***Expanding the Tree*** (on page 83).
2. Click the outlet you want in the Dominion PX Explorer pane. The page specific to that outlet opens in the right pane.
3. Click Setup in the Settings section. The setup dialog for the selected outlet appears.

Tip: When the Outlets folder is selected, you can also trigger the same dialog by highlighting the outlet on the Outlets page and then clicking Setup.

4. In the Threshold Configuration table, click the sensor whose thresholds you want to configure.
5. Click Edit. A threshold setup dialog for the selected sensor appears.

Tip: You can also double-click the desired sensor in the Threshold Configuration table to trigger this dialog.

6. Configure the Lower Critical, Lower Warning, Upper Warning and Upper Critical thresholds respectively.
   - To enable any threshold, select the corresponding checkbox. To disable a threshold, deselect the checkbox.
   - After any threshold is enabled, type an appropriate numeric value in the accompanying text box.
7. To enable the deassertion hysteresis for all thresholds, type a numeric value other than zero in the Deassertion Hysteresis field. See ***What is Deassertion Hysteresis?*** (on page 178).
8. To enable the assertion timeout for all thresholds, type a numeric value other than zero in the Assertion Timeout (samples) field. See ***What is Assertion Timeout?*** (on page 179).
9. Click OK in the threshold setup dialog to retain the changes.
10. To set the thresholds for other sensors, repeat Steps 4 to 9.
11. Click OK to save the changes.

Important: The final step is required or the threshold changes are not saved.

Bulk Configuration for Outlet Thresholds

The PX allows you to set the power thresholds for multiple outlets at a time so that you can save time when configuring a number of outlet thresholds.

Note: To set the power thresholds for an individual outlet, you can either follow the instructions below or those described in the section **Setting an Outlet's Thresholds** *(on page 173).*

To configure thresholds, deassertion hysteresis and assertion timeout for multiple outlets:

1. If the PDU folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 83).

Note: The PDU folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the PDU** *(on page 98).*

2. Click the Outlets folder. The Outlets page opens.

3. Click Bulk Setup. The Outlet Threshold Bulk Setup dialog appears, with a list of all outlets.
4. In the Show Outlet Sensors of Type field, select the type of power thresholds you want to configure.
5. Select desired outlets by having their corresponding checkboxes selected.
   - To select all outlets, select the checkbox labeled Sensor in the header row, and all checkboxes are selected.
   - To select partial outlets, select the corresponding checkboxes of those outlets by clicking on their checkboxes.
   - To deselect any outlet, just click on the checkbox once again.
6. Click Edit Thresholds. The threshold bulk setup dialog appears.
7. Configure the Lower Critical, Lower Warning, Upper Warning and Upper Critical thresholds respectively.
   - To enable any threshold, select the corresponding checkbox. To disable a threshold, deselect the checkbox.
   - After any threshold is enabled, type an appropriate numeric value in the accompanying text box.
8. To enable the deassertion hysteresis for all thresholds, type a numeric value other than zero in the Deassertion Hysteresis field. See ***What is Deassertion Hysteresis?*** (on page 178).
9. To enable the assertion timeout for all thresholds, type a numeric value other than zero in the Assertion Timeout (samples) field. See ***What is Assertion Timeout?*** (on page 179).
10. Click OK to save the changes.

Setting Inlet Thresholds

You can set the inlet thresholds so that the alerts are generated when the inlet current and/or voltage crosses the thresholds.

To set the inlet thresholds:

1. If the PDU folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 83).

   Note: The PDU folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the PDU** *(on page 98).*

2. Click Inlet I1 in the Dominion PX Explorer pane, and the Inlet I1 page opens in the right pane.
3. Click Setup. The Inlet I1 Setup dialog appears.
4. In the Threshold Configuration table, click the sensor whose thresholds you want to configure.

5. Click Edit. A threshold setup dialog for the selected sensor appears.

   Tip: You can also double-click the desired sensor in the Threshold Configuration table to trigger this dialog.

6. Configure the Lower Critical, Lower Warning, Upper Warning and Upper Critical thresholds respectively.
   - To enable any threshold, select the corresponding checkbox. To disable a threshold, deselect the checkbox.
   - After any threshold is enabled, type an appropriate numeric value in the accompanying text box.
7. To enable the deassertion hysteresis for all thresholds, type a numeric value other than zero in the Deassertion Hysteresis field. See ***What is Deassertion Hysteresis?*** (on page 178).
8. To enable the assertion timeout for all thresholds, type a numeric value other than zero in the Assertion Timeout (samples) field. See ***What is Assertion Timeout?*** (on page 179).
9. Click OK in the threshold setup dialog to retain the changes.
10. To set the thresholds for other sensors, repeat Steps 4 to 9.
11. Click OK to save the changes.

Important: The final step is required or the threshold changes are not saved.

Setting a Circuit Breaker's Thresholds

Setting the circuit breaker thresholds enables the PDU to generate alerts when any circuit breaker crosses the thresholds.

To set the thresholds for a circuit breaker:

1. Expand the Overcurrent Protectors folder to show all circuit breakers in the Dominion PX Explorer pane. See ***Expanding the Tree*** (on page 83).

   Note: The PDU folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the PDU** *(on page 98).*

2. Click the desired circuit breaker in the Dominion PX Explorer pane, and the page for this circuit breaker opens in the right pane.
3. Click Setup. The Overcurrent Protector Setup dialog appears.
4. In the Threshold Configuration table, click the sensor whose thresholds you want to configure.
5. Click Edit. A threshold setup dialog for the selected sensor appears.

Tip: You can also double-click the desired sensor in the Threshold Configuration table to trigger this dialog.

6. Configure the Lower Critical, Lower Warning, Upper Warning and Upper Critical thresholds respectively.
   - To enable any threshold, select the corresponding checkbox. To disable a threshold, deselect the checkbox.
   - After any threshold is enabled, type an appropriate numeric value in the accompanying text box.
7. To enable the deassertion hysteresis for all thresholds, type a numeric value other than zero in the Deassertion Hysteresis field. See ***What is Deassertion Hysteresis?*** (on page 178).
8. To enable the assertion timeout for all thresholds, type a numeric value other than zero in the Assertion Timeout (samples) field. See ***What is Assertion Timeout?*** (on page 179).
9. Click OK to save the changes.

Bulk Configuration for Circuit Breaker Thresholds

The PX allows you to set the power thresholds for multiple circuit breakers at a time so that you can save time when configuring a number of circuit breaker thresholds.

Note: To set the power thresholds for an individual circuit breaker, you can either follow the instructions below or those described in the section **Setting a Circuit Breaker's Thresholds** *(on page 176).*

To configure thresholds, deassertion hysteresis and assertion timeout for multiple circuit breakers:

1. If the PDU folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 83).

   Note: The PDU folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the PDU** *(on page 98).*

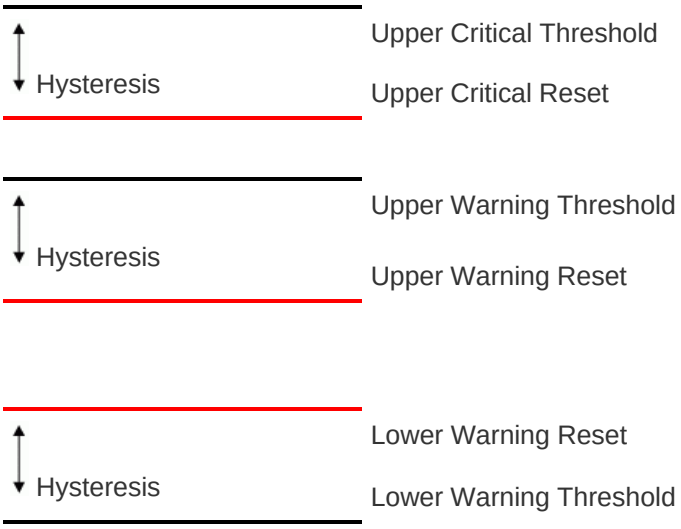
2. Click the Overcurrent Protectors folder. The Overcurrent Protectors page opens.
3. Click Bulk Setup. The Overcurrent Protector Threshold Bulk Setup dialog appears, with a list of all circuit breakers.
4. Select desired circuit breakers by having their corresponding checkboxes selected.
   - To select all circuit breakers, select the checkbox labeled Sensor in the header row, and all checkboxes are selected.

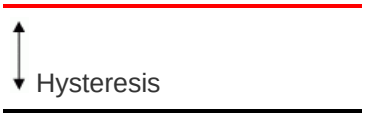
- To select partial circuit breakers, select the corresponding checkboxes of those circuit breakers by clicking on their checkboxes.
- To deselect any circuit breaker, just click on the checkbox once again.

5. Click Edit Thresholds. The threshold bulk setup dialog appears.
6. Configure the Lower Critical, Lower Warning, Upper Warning and Upper Critical thresholds respectively.
   - To enable any threshold, select the corresponding checkbox. To disable a threshold, deselect the checkbox.
   - After any threshold is enabled, type an appropriate numeric value in the accompanying text box.
7. To enable the deassertion hysteresis for all thresholds, type a numeric value other than zero in the Deassertion Hysteresis field. See ***What is Deassertion Hysteresis?*** (on page 178).
8. To enable the assertion timeout for all thresholds, type a numeric value other than zero in the Assertion Timeout (samples) field. See ***What is Assertion Timeout?*** (on page 179).
9. Click OK to save the changes.

What is Deassertion Hysteresis?

The hysteresis setting determines when a threshold condition is reset. This diagram illustrates how hysteresis values relate to thresholds:





The hysteresis values define a reset threshold. For upper thresholds, the measurement must fall past this reset threshold before a deassertion event is generated. For lower thresholds, the measurement must rise above this reset threshold before a deassertion event is generated.

Example: When Hysteresis is Useful

This example demonstrates when a deassertion hysteresis is useful.

The current critical threshold for the inlet is set to 19 amps (A). The current draw rises to 20A, triggering a Current Critical alert. The current then continues to fluctuate between 18.1A and 20A.

With the hysteresis set to 1A, PX continues to indicate that the current on the inlet is above critical. Without hysteresis (that is, the hysteresis is set to zero), PX would de-assert the condition each time the current dropped to 18.9A, and re-assert the condition each time the current reached 19A or higher. With the fluctuating current, this could result in a number of repeating SNMP traps, and/or an e-mail account full of repeating SMTP alert notifications.

Example: When to Disable Hysteresis

This is an example of when you want to disable the use of hysteresis for outlets. Hysteresis is disabled when its value is set to zero.

The upper warning threshold for current in Outlet 2 is set to 8A. In normal usage, Outlet 2 draws 7.6A of current. A spike in demand causes the current to reach 9A, triggering an alert. The current then settles to the normal draw of 7.6A.

With the hysteresis disabled (that is, set to zero), the PX de-asserts the condition once the current drops to 7.9A. Otherwise the outlet would still be considered above the warning threshold as long as the current never dropped to 7.0A while the hysteresis was set to 1. The condition would not de-assert, even if the current draw returned to normal.

What is Assertion Timeout?

When the assertion timeout is enabled, the PX device asserts any warning or critical condition only after a specified number of consecutive samples that cross a particular threshold are generated. This prevents a number of threshold alerts from being generated if the measurements return to normal immediately after rising above any upper threshold or dropping below any lower threshold.

Event Rules and Actions

A benefit of the product's intelligence is its ability to notify you of and react to a change in conditions. This event notification or reaction is an "event rule."

The PX is shipped with two built-in event rules, which cannot be deleted.

- System Event Log Rule: This causes ANY event occurred to the PX to be recorded in the internal log. It is enabled by default.
- System SNMP Notification Action: This causes SNMP traps or informs to be sent to specified IP addresses or hosts when ANY event occurs to the PX. It is disabled by default.

If these two do not satisfy your needs, you can create additional rules to respond to different events.

Note: Internet Explorer® 8 (IE8) does not use compiled JAVA script. When using IE8 to create or change event rules, the CPU performance may be degraded, resulting in the appearance of the connection time out message. When this occurs, click Ignore to continue.

Components of an Event Rule

An event rule defines what the PX does in certain situations and is composed of two parts:

- Event: This is the situation where the PX or part of it meets a certain condition. For example, the inlet's voltage exceeds the warning threshold.
- Action: This is the response to the event. For example, the PX notifies the system administrator of the event and records the event in the log.

Creating an Event Rule

The best way to create a new set of event rules in sequence is to:

- Create actions for responding to one or multiple events
- Create rules to determine what actions are taken when these events occur

Creating Actions

The PX comes with two built-in actions:

- System Event Log Action: This action records the selected event in the internal log when the event occurs.
- System SNMP Notification Action: This action sends SNMP notifications to one or multiple IP addresses after the selected event occurs.

Note: No IP addresses are specified for the "System SNMP Notification Action" by default so you must specify IP addresses before applying this action to any event rule.

The default actions cannot be deleted.

To create new actions:

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting from 1.
5. In the Action field, click the Action drop-down arrow and select the desired action:

Action	Function
Execute an action group	Creates a group of actions comprising existing actions. See ***Action Group*** (on page 183).
Log event message	Records the selected events in the internal log. See ***Log an Event Message*** (on page 184).
Request LHX Maximum Cooling	Applies the maximum cooling to the LHX device. See ***Request LHX Maximum Cooling*** (on page 184). This option is available only when the Schroff LHX support has been enabled.
Send Snapshots via SMTP	Emails the snapshots captured by a connected Logitech® webcam (if available). See ***Send a Snapshot via Email*** (on page 184).
Send SMTP message	Emails a textual message. See ***Send EMail*** (on page 186).

Action	Function
Send SNMP notification	Sends SNMP traps or informs to one or multiple SNMP destinations. See ***Send an SNMP Notification*** (on page 187).
Syslog message	Makes the PX automatically forward event messages to the specified syslog server. See ***Syslog Message*** (on page 189).
Send SMS message	Sends an English message to a mobile phone. See ***Send SMS Message*** (on page 191).
Switch LHX	Switches on or off the LHX device. See ***Switch LHX*** (on page 192). This option is available only when the Schroff LHX support has been enabled.
Record Snapshots to Webcam Storage	Starts or stops a connected webcam from taking snapshots. See ***Record Snapshots to Webcam Storage*** (on page 193).
Change load shedding state	Enters or quits the load shedding mode. See ***Change Load Shedding State*** (on page 190).
Switch outlet	Switches on, off or cycles the power to the specified outlet(s). See ***Switch Outlets*** (on page 192).

Note: The "Change load shedding state" and "Switch outlet" options are only available for outlet-switching capable PDUs.

6. Click Save to save the new action.

Note: If you do not click Save before quitting the current settings page, a message appears. Then click Yes to save the changes, Discard to abort or Cancel to return to the current settings page.

7. To create additional actions, repeat the above steps.
8. Click Close to quit the dialog.

Action Group

You can create an action group that performs up to 32 actions. After creating such an action group, you can easily assign this set of actions to an event rule rather than selecting all needed actions one by one per rule.

Note: A supported modem, such as the Cinterion® GSM MC52i modem, must be plugged in to the PX in order to send SMS messages.

To create an action group:

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting from 1.
5. In the Action field, click the Action drop-down arrow and select the desired action: Execute an action group.
6. To mark an action as part of the action group, select it from the Available Actions list box, and click to move it to the Used Actions list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

   To move all actions to the Used Actions list box at a time, click . A maximum of 32 actions can be grouped.
7. To remove an action from the action group, select it from the Used Actions list box, and click to move it to the Available Actions list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

   To remove all actions at a time, click .
8. Click Save to save the new action.

   Note: If you do not click Save before quitting the current settings page, a message appears. Then click Yes to save the changes, Discard to abort or Cancel to return to the current settings page.
9. To create additional action groups, repeat Steps 3 to 8.

Log an Event Message

This option records the selected events in the internal log.

To create a log event message:

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting from 1.
5. In the Action field, click the Action drop-down arrow and select the desired action: Log event message.
6. Click OK to save the new action.
7. Click Close to quit the dialog.

Request LHX Maximum Cooling

If Schroff LHX Support is enabled, the LHX-related actions will be available. See ***Enabling and Disabling Schroff LHX Heat Exchanger Support*** (on page 252).

The "Request LHX Maximum Cooling" action applies the maximum cooling to the LHX device.

To request maximum cooling for LHX:

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting from 1.
5. In the Action field, click the Action drop-down arrow and select the desired action: Request LHX Maximum Cooling.

Send a Snapshot via Email

This option notifies one or multiple persons of the selected events by emailing snapshots or videos captured by a connected Logitech® webcam.

To create a send snapshot via email action:

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting from 1.
5. In the Action field, click the Action drop-down arrow and select the desired action: Send Snapshots via SMTP.
6. In the "Recipients email addresses" field, specify the email address(es) of the recipient(s). Use a comma to separate multiple email addresses.
7. To use the SMTP server specified in the SMTP Server Settings dialog, select the Use Default SMTP Server checkbox.
8. To use a different SMTP server, select the Use Custom SMTP Settings checkbox. If the SMTP server settings are not configured yet, click Configure. See ***Configuring the SMTP Settings*** (on page 117) for the information of each field.
9. Select the webcam that is capturing the images you want sent in the email.
10. Use the slide bars to increase or decrease the following:
    - Number of Snapshots - the number of snapshots to be included in the sequence of images that are taken when the event occurs. For example, you can specify 10 images be taken once the event triggers the action.
    - Snapshots/Mail field - the number of snapshots from the sequence to be sent at one time in the email.
    - "Time before first Snapshot (s):" - the amount of time (in seconds) between when the event is triggered and the webcam begins taking snapshots.
    - "Time between Snapshots (s):" - the amount of time between when each snapshot is taken.
11. Click OK to save the new action.
12. Click Close to quit the dialog.

Send EMail

You can configure emails to be sent when an event occurs and can customize the message.

Messages consist of a combination of free text and PX placeholders. The placeholders represent information is pulled from the PX and inserted into the message.

For example:

```
[USERNAME] logged into the device on [TIMESTAMP]
```

translates to

```
JQPublic logged into the device on 2012-January-30 21:00
```

See ***Email and SMS Message Placeholders*** (on page 206) for a list and definition of available variables.

To configure sending emails:

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting from 1.
5. In the Action field, click the Action drop-down arrow and select the desired action: Send SMTP message.
6. In the "Recipients email addresses" field, specify the email address(es) of the recipient(s). Use a comma to separate multiple email addresses.
7. To use the SMTP server specified in the SMTP Server Settings dialog, select the Use Default SMTP Server checkbox.

   To use a different SMTP server, select the Use Custom SMTP Settings checkbox.

   If the SMTP server settings are not configured yet, click Configure. See ***Configuring the SMTP Settings*** (on page 117) for the information of each field. Default messages are sent based on the event. See ***Default Log Messages*** (on page 198) for a list of default log messages and events that trigger them.
8. If needed, select the Use Custom Log Message checkbox, and then create a custom message in the provided field.

Click the Information icon to open the Event Context Information dialog, which contains a list of placeholders and their definitions. See ***Email and SMS Message Placeholders*** (on page 206) for more details.

9. Click OK to save the new action.
10. Click Close to quit the dialog.

Send an SNMP Notification

This option sends an SNMP notification to one or multiple SNMP destinations.

To configure sending an SNMP notification:

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting from 1.
5. In the Action field, click the Action drop-down arrow and select the desired action: Send SNMP notification.
6. Select the type of SNMP notification. See either procedure below according to your selection.

To send SNMP v2c notifications:

1. From the Notification Type drop-down, select SNMP v2c Trap or SNMP v2c Inform.
2. For SNMP INFORM communications, leave the resend settings at their default or:
   a. In the Timeout (sec) field, enter the interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.
   b. In the Number of Retries field, enter the number of times you want to resend the inform communication if it fails. For example, inform communications are resent up to 5 times when the initial communication fails.
3. In the Host fields, enter the IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP system agent.
4. In the Port fields, enter the port number used to access the device(s).

5. In the Community fields, enter the SNMP community string to access the device(s). The community is the group representing the PX and all SNMP management stations.

To send SNMP v3 notifications:

1. From the Notification Type drop-down, select SNMP v3 Trap or SNMP v3 Inform.
2. For SNMP TRAPs, the engine ID is prepopulated.
3. For SNMP INFORM communications, leave the resend settings at their default or:
   a. In the Timeout (sec) field, enter the interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.
   b. In the Number of Retries field, enter the number of times you want to resend the inform communication if it fails. For example, inform communications are resent up to 5 times when the initial communication fails.
4. For both SNMP TRAPS and INFORMS, enter the following as needed and then click OK to apply the settings:
   a. Host name
   b. Port number
   c. User ID needed to access the host
   d. Select the host security level

Security level	Description
"noAuthNoPriv"	Select this if no authorization or privacy protocols are needed. • Click OK
"authNoPriv"	Select this if authorization is required but no privacy protocols are required. • Select the authentication protocol - MD5 or SHA • Enter the authentication passphrase and then confirm the authentication passphrase • Click OK
"authPriv"	Select this if authentication and privacy protocols are required. • Select the authentication protocol - MD5 or SHA • Enter the authentication passphrase and confirm the authentication passphrase • Select the Privacy Protocol - DES or AES • Enter the privacy passphrase and then confirm the privacy passphrase • Click OK

Syslog Message

Use this action to automatically forward event messages to the specified syslog server.

To configure a syslog message action:

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting from 1.
5. In the Action field, click the Action drop-down arrow and select the desired action: Syslog message.
6. In the "Syslog server" field, specify the IP address to which the syslog is forwarded.
7. In the Port field, specify an appropriate port number.

8. Click OK to save the new action.
9. Click Close to quit the dialog.

Change Load Shedding State

The "Change load shedding state" action is available only when your PDU is able to control outlet power. Use this action to activate or deactivate the load shedding mode for responding to a specific event. See ***Setting Non-Critical Outlets and Load Shedding Mode*** (on page 167) for additional information.

To change the load shedding state:

1. Click the Actions tab.
2. Click New.
3. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting from 1.
4. In the Action field, click the Action drop-down arrow and select the desired action: Change load shedding state.
5. From the Operation drop-down, select either of the following:
   - Enable load shedding: Enters the load shedding mode when the specified event occurs.
   - Disable load shedding: Quits the load shedding mode when the specified event occurs.
6. Click OK to save the new action.
7. Click Close to quit the dialog.

Send SMS Message

You can configure emails to be sent when an event occurs and can customize the message.

Messages consist of a combination of free text and PX placeholders. The placeholders represent information is pulled from the PX and inserted into the message.

A supported modem, such as the Cinterion® GSM MC52i modem, must be plugged in to the PX in order to send SMS messages.

Note: The PX cannot receive SMS messages.

For example:

```
[USERNAME] logged into the device on [TIMESTAMP]
```

translates to

```
JQPublic logged into the device on 2012-January-30 21:00
```

See ***Email and SMS Message Placeholders*** (on page 206) for a list and definition of available variables.

To configure SMS message:

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting from 1.
5. In the Action field, click the Action drop-down arrow and select the desired action: Send SMS message.
6. In the Recipients Phone Number field, specify the phone number of the recipient.
7. Select the Use Custom Log Message checkbox, then create a custom message in the provided field.

   Click the Information icon to open the Event Context Information dialog, which contains a list of placeholders and their definitions. See ***Email and SMS Message Placeholders*** (on page 206) for more details.

   Note: Only English is supported for SMS messages. For Turkish characters, use 7-bit ASCII instead.
8. Click OK to save the new action.
9. Click Close to quit the dialog.

Switch LHX

If Schroff LHX Support is enabled, the LHX-related actions will be available. See ***Enabling and Disabling Schroff LHX Heat Exchanger Support*** (on page 252).

Use this action to switch the LHX on or off when, for example, temperature thresholds are reached.

To create a switch LHX action:

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting from 1.
5. In the Action field, click the Action drop-down arrow and select the desired action: Switch LHX.
6. From the Operation drop-down, select Turn LHX On or Turn LHX Off.
7. From the Available LHXs list box, click on the LHX to be turned on or off, then click or to add to the Switched LHXs list box. Use or to remove the LHX from the Switched LHXs list box, thereby removing the action.
8. Click OK to save the new action.
9. Click Close to quit the dialog.

Switch Outlets

The "Switch outlets" action is available only when your PDU is outlet-switching capable. This action turns on, off or power cycles a specific outlet.

To switch on, off or power cycle any outlet(s):

1. Click the Actions tab.
2. Click New.
3. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting from 1.
4. In the Action field, click the Action drop-down arrow and select the desired action: Switch outlets.

5. From the Operation drop-down, select an operation for the selected outlet(s).
   - Turn Outlet On: Turns on the selected outlet(s).
   - Turn Outlet Off: Turns off the selected outlet(s).
   - Cycle Outlet: Cycles power to the selected outlet(s).
6. To select the outlet where this action will be applied, select it from the Available Outlets list and click to add it to the Switched Outlets list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

   To move all outlets to the Switched Outlets list box at a time, click .
7. To remove any outlet from the Switched Outlets list, select it from the Switched Outlets list and click to move it to the Available Outlets list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

   To remove all outlets at a time, click .
8. Click OK to save the new action.
9. Click Close to quit the dialog.

Record Snapshots to Webcam Storage

This option allows you to define an action that starts or stops a specific webcam from taking snapshots.

To configure a record snapshot to webcam storage action:

1. Choose Device Settings > Event Rules. The Event Rules Settings dialog opens.
2. Click the Actions tab.
3. Click New.
4. In the "Action name" field, type a new name for the action. The default name is New Action <number>, where <number> is a sequential number starting from 1.
5. In the Action field, click the Action drop-down arrow and select the desired action: Record Snapshots to Webcam Storage.
6. Select a webcam from the Webcam drop-down.
7. Selecting the action to perform - Start recording or Stop recording. If "Start recording" is selected, do the following:
   a. Use the slide bar to specify the total number of snapshots to be taken when the event occurs. The maximum amount of snapshots that can be stored on the PX is ten (10). If you set it for a number greater than ten, after the tenth snapshot is taken and stored, the oldest snapshots are overwritten.

b. In the "Time before first Snapshot (s):" field, use the slide bar to specify the amount of time (in seconds) between when the event is triggered and the webcam begins taking snapshots.

c. In the "Time between Snapshots (s):" field, use the slide bar to specify the amount of time between when each snapshot is taken.

8. Click OK to save the new action.
9. Click Close to quit the dialog.

Creating Rules

After required actions are available, you can create event rules to determine what actions are taken to respond to specific events.

By default, the PX provides two built-in event rules -- System Event Log Rule and System SNMP Notification Action. If the built-in rules do not satisfy your needs, create new ones.

To create event rules:

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. On the Rules tab, click New.
3. In the "Rule name" field, type a new name for identifying the rule. The default name is New Rule <number>, where <number> is a sequential number.
4. Select the Enable checkbox to enable the SNMP notification feature.
5. Click Event to select an event for which you want to trigger an action. A pull-down menu showing various types of events appears.
   - Select the desired event type from the pull-down menu, and if a submenu appears, continue the navigation until the desired event is selected.

   Note: The option <Any sub-event> refers to all events/items listed on the same submenu, <Any slot> refers to all slots, <Any server> refers to all servers, and <Any user> refers to all users.

6. According to the event you selected in the previous step, the "Trigger condition" field containing three radio buttons may or may not appear.

Event types	Radio buttons
Numeric sensor threshold-crossing events, or the occurrence of the selected event -- true or false	Available radio buttons include "Asserted," "Deasserted" and "Both." ▪ Asserted: The PX takes the action only when the event occurs. This means the status of the described event transits from FALSE to TRUE. ▪ Deasserted: The PX takes the action only when the event condition disappears. This means the status of the described event transits from TRUE to FALSE. ▪ Both: The PX takes the action both when the event occurs (asserts) and when the event condition disappears (deasserts). • For connection state for USB cascading and auxiliary/RS-485 devices, assertion is displayed as "connected" and deassertion as "disconnected"
Discrete (on/off) sensor state change	Available radio buttons include "Alarmed," "No longer alarmed" and "Both." ▪ Alarmed: The PX takes the action only when the chosen sensor enters the alarmed state, that is, the abnormal state. ▪ No longer alarmed: The PX takes the action only when the chosen sensor returns to normal. ▪ Both: The PX takes the action both when the chosen sensor enters or quits the alarmed state.
Sensor availability	Available radio buttons include "Unavailable," "Available" and "Both." ▪ Unavailable: The PX takes the action only when the chosen sensor is NOT detected and becomes unavailable. ▪ Available: The PX takes the action only when the chosen sensor is detected and becomes available. ▪ Both: The PX takes the action both when the chosen sensor becomes unavailable or available.

Event types	Radio buttons
Network interface link state	Available radio buttons include "Link state is up," "Link state is down" and "Both." ▪ Link state is up: The PX takes the action only when the network link state changes from down to up. ▪ Link state is down: The PX takes the action only when the network link state changes from up to down. ▪ Both: The PX takes the action whenever the network link state changes.
Function enabled or disabled	Available radio buttons include "Enabled," "Disabled" and "Both." ▪ Enabled: The PX takes the action only when the chosen function is enabled. ▪ Disabled: The PX takes the action only when the chosen function is disabled. ▪ Both: The PX takes the action when the chosen function is either enabled or disabled.
User logon state	Available radio buttons include "Logged in," "Logged out," and "Both." ▪ Logged in: The PX takes the action only when the selected user logs in. ▪ Logged out: The PX takes the action only when the selected user logs out. ▪ Both: The PX takes the action both when the selected user logs in and logs out.
Server monitoring event	Available radio buttons include "Monitoring started," "Monitoring stopped," and "Both." ▪ Monitoring started: The PX takes the action only when the monitoring of any specified server starts. ▪ Monitoring stopped: The PX takes the action only when the monitoring of any specified server stops. ▪ Both: The PX takes the action when the monitoring of any specified server starts or stops.

Event types	Radio buttons
Server reachability	Available radio buttons include "Unreachable," "Reachable," and "Both." ▪ Unreachable: The PX takes the action only when any specified server becomes inaccessible. ▪ Reachable: The PX takes the action only when any specified server becomes accessible. ▪ Both: The PX takes the action when any specified server becomes either inaccessible or accessible.
Connection or disconnection of a device, such as the RF Code tag or a subsequent slave device	Available radio buttons include "Connected," "Disconnected" and "Both." ▪ Connected: PX takes the action only when the selected device is physically connected to it. ▪ Disconnected: PX takes the action only when the selected device is physically disconnected from it. ▪ Both: PX takes the action both when the selected device is physically connected to it and when it is disconnected.
Outlet power state change	Available radio buttons include "On," "Off" and "Both." ▪ On: PX takes the action only when the chosen outlet is turned ON. ▪ Off: PX takes the action only when the chosen outlet is turned OFF. ▪ Both: PX takes the action when the chosen outlet is either turned ON or turned OFF.

Note: The outlet power state change events are available only for outlet-switching capable PDUs.

1. In the Actions field, select the desired action from the "Available actions" list box, and click the Add button to move the selected action to the "Selected actions" list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

   To add all actions at a time, simply click the Add All button.

   If the desired action is not available yet, click Create New Action to immediately create it. Upon complete, the newly-created action is moved to the "Selected actions" list box.

- To remove any action, select it from the "Selected actions" list box, and click the Remove button to move it back to the "Available actions" list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.

To remove all actions at a time, simply click the Remove All button.

2. Click Save to save the new event rule.

Note: If you do not click Save before quitting the current settings page, a message appears. Then click Yes to save the changes, Discard to abort or Cancel to return to the current settings page.

3. Repeat Steps 2 to 10 to create additional event rules.
4. Click Close to quit the dialog.

Default Log Messages

Following are default log messages triggered and emailed to specified recipients when PX events occur (are TRUE) or, in some cases, do not occur (are FALSE). See ***Send EMail*** (on page 186) for information configuring email messages to be sent when specified events occur.

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
Device > System started	System started.	
Device > System reset	System reset performed by user '[USERNAME]' from host '[USERIP]'.	
Device > Firmware validation failed	Firmware validation failed by user '[USERNAME]' from host '[USERIP]'.	
Device > Firmware update started	Firmware upgrade started from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.	
Device > Firmware update completed	Firmware upgraded successfully from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.	
Device > Firmware update failed	Firmware upgrade failed from version '[OLDVERSION]' to version '[VERSION]' by user '[USERNAME]' from host '[USERIP]'.	
Device > Device identification changed	Config parameter '[PARAMETER]' changed to '[VALUE]' by user '[USERNAME]' from host '[USERIP]'.	

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
Device > Device settings saved	Device settings saved from host '[USERIP]'	
Device > Device settings restored	Device settings restored from host '[USERIP]'	
Device > Event log cleared	Event log cleared by user '[USERNAME]' from host '[USERIP]'.	
Device > Bulk configuration saved	Bulk configuration saved from host '[USERIP]'.	
Device > Bulk configuration copied	Bulk configuration copied from host '[USERIP]'.	
Device > Network interface link state is up	The [IFNAME] network interface link is now up.	The [IFNAME] network interface link is now down.
Device > Sending SMTP message failed	Sending SMTP message to '[RECIPIENTS]' using server '[SERVER]' failed.	
Device > An LDAP error occurred	An LDAP error occurred: [LDAPERRORDESC].	
Device > An Radius error occurred	An Radius error occurred: [RADIUSERRORDESC].	
Device > USB slave connected	USB slave connected.	USB slave disconnected.
Device > Features > Schroff LHX Support	Schroff LHX support enabled.	Schroff LHX support disabled.
User Administration > User added	User '[TARGETUSER]' added by user '[USERNAME]' from host '[USERIP]'.	
User Administration > User modified	User '[TARGETUSER]' modified by user '[USERNAME]' from host '[USERIP]'.	
User Administration > User deleted	User '[TARGETUSER]' deleted by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Password changed	Password of user '[TARGETUSER]' changed by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Password settings changed	Password settings changed by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Role added	Role '[TARGETROLE]' added by user '[USERNAME]' from host '[USERIP]'.	
User Administration > Role modified	Role '[TARGETROLE]' modified by user '[USERNAME]' from host	

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
	'[USERIP]'.	
User Administration > Role deleted	Role '[TARGETROLE]' deleted by user '[USERNAME]' from host '[USERIP]'.	
User Activity > * > User logon state	User '[USERNAME]' from host '[USERIP]' logged in.	User '[USERNAME]' from host '[USERIP]' logged out.
User Activity > * > Authentication failure	Authentication failed for user '[USERNAME]' from host '[USERIP]'.	
User Activity > * > User accepted the Restricted Service Agreement	User '[USERNAME]' from host '[USERIP]" accepted the Restricted Service Agreement.	User '[USERNAME]' from host '[USERIP]" declined the Restricted Service Agreement.
User Activity > * > User blocked	User '[USERNAME]' from host '[USERIP]' was blocked.	
User Activity > * > Session timeout	Session of user '[USERNAME]' from host '[USERIP]' timed out.	
PDU > Load Shedding > Enabled	PX placed in Load Shedding Mode by user '[USERNAME]' from host '[USERIP]'.	PX removed from Load Shedding Mode by user '[USERNAME]' from host '[USERIP]'.
Inlet > * > Sensor > * > Unavailable	Sensor '[INLETSENSOR]' on inlet '[INLET]' unavailable.	Sensor '[INLETSENSOR]' on inlet '[INLET]' available.
Inlet > * > Sensor > * > Above upper critical threshold	Sensor '[INLETSENSOR]' on inlet '[INLET]' asserted 'above upper critical'.	Sensor '[INLETSENSOR]' on inlet '[INLET]' deasserted 'above upper critical'.
Inlet > * > Sensor > * > Above upper warning threshold	Sensor '[INLETSENSOR]' on inlet '[INLET]' asserted 'above upper warning'.	Sensor '[INLETSENSOR]' on inlet '[INLET]' deasserted 'above upper warning'.
Inlet > * > Sensor > * > Below lower warning threshold	Sensor '[INLETSENSOR]' on inlet '[INLET]' asserted 'below lower warning'.	Sensor '[INLETSENSOR]' on inlet '[INLET]' deasserted 'below lower warning'.
Inlet > * > Sensor > * > Below lower critical threshold	Sensor '[INLETSENSOR]' on inlet '[INLET]' asserted 'below lower critical'.	Sensor '[INLETSENSOR]' on inlet '[INLET]' deasserted 'below lower critical'.
Inlet > * > Pole > * > Sensor > * > Unavailable	Sensor '[POLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' unavailable.	Sensor '[POLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' available.
Inlet > * > Pole > * > Sensor > * > Above upper critical threshold	Sensor '[POLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' asserted 'above upper critical'.	Sensor '[POLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' deasserted 'above upper critical'.
Inlet > * > Pole > * > Sensor > * > Above upper warning threshold	Sensor '[POLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]'	Sensor '[POLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]'

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
	asserted 'above upper warning'.	deasserted 'above upper warning'.
Inlet > * > Pole > * > Sensor > * > Below lower warning threshold	Sensor '[POLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' asserted 'below lower warning'.	Sensor '[POLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' deasserted 'below lower warning'.
Inlet > * > Pole > * > Sensor > * > Below lower critical threshold	Sensor '[POLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' asserted 'below lower critical'.	Sensor '[POLESENSOR]' on pole '[INLETPOLE]' of inlet '[INLET]' deasserted 'below lower critical'.
Outlet > * > Power control > Powered on	Outlet '[OUTLET]' has been powered on by user '[USERNAME]' from host '[USERIP]'.	
Outlet > * > Power control > Powered off	Outlet '[OUTLET]' has been powered off by user '[USERNAME]' from host '[USERIP]'.	
Outlet > * > Power control > Power cycled	Outlet '[OUTLET]' power cycle initiated by user '[USERNAME]' from host '[USERIP]'.	
Outlet > * > Sensor > * > Unavailable	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' unavailable.	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' available.
Outlet > * > Sensor > * > Above upper critical threshold	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' asserted 'above upper critical'.	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' deasserted 'above upper critical'.
Outlet > * > Sensor > * > Above upper warning threshold	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' asserted 'above upper warning'.	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' deasserted 'above upper warning'.
Outlet > * > Sensor > * > Below lower warning threshold	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' asserted 'below lower warning'.	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' deasserted 'below lower warning'.
Outlet > * > Sensor > * > Below lower critical threshold	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' asserted 'below lower critical'.	Sensor '[OUTLETSENSOR]' on outlet '[OUTLET]' deasserted 'below lower critical'.
Outlet > * > Sensor > * > On	Outlet '[OUTLET]' state changed to on.	Outlet '[OUTLET]' state changed to off.
Outlet > * > Pole > * > Sensor > Unavailable	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' unavailable.	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' available.
Outlet > * > Pole > * > Sensor > Above upper critical threshold	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' asserted 'above upper critical'.	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' deasserted 'above upper critical'.
Outlet > * > Pole > * > Sensor >	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]'	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet

Event/Context	Default Assertion Message when the Event = TRUE	Default Assertion Message when the Event = FALSE*
Above upper warning threshold	asserted 'above upper warning'.	'[OUTLET]' deasserted 'above upper warning'.
Outlet > * > Pole > * > Sensor > Below lower warning threshold	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' asserted 'below lower warning'.	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' deasserted 'below lower warning'.
Outlet > * > Pole > * > Sensor > Below lower critical threshold	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' asserted 'below lower critical'.	Sensor '[POLESENSOR]' on pole '[OUTLETPOLE]' of outlet '[OUTLET]' deasserted 'below lower critical'.
Overcurrent Protector > * > Sensor > * > Unavailable	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' unavailable.	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' available.
Overcurrent Protector > * > Sensor > * > Above upper critical threshold	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' asserted 'above upper critical'.	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' deasserted 'above upper critical'.
Overcurrent Protector > * > Sensor > * > Above upper warning threshold	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' asserted 'above upper warning'.	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' deasserted 'above upper warning'.
Overcurrent Protector > * > Sensor > * > Below lower warning threshold	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' asserted 'below lower warning'.	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' deasserted 'below lower warning'.
Overcurrent Protector > * > Sensor > * > Below lower critical threshold	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' asserted 'below lower critical'.	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' deasserted 'below lower critical'.
Overcurrent Protector > * > Sensor > * > Open/Closed	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' is open.	Sensor '[OCPSENSOR]' on overcurrent protector '[OCP]' is closed.
External Sensor Slot > * > Numeric Sensor > Unavailable	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' unavailable.	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' available.
External Sensor Slot > * > Numeric Sensor > Above upper critical threshold	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'above upper critical'.	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'above upper critical'.
External Sensor Slot > * > Numeric Sensor > Above upper warning threshold	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'above upper warning'.	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'above upper warning'.

External Sensor Slot > * > Numeric Sensor > Below lower warning threshold	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'below lower warning'.	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'below lower warning'.
External Sensor Slot > * > Numeric Sensor > Below lower critical threshold	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' asserted 'below lower critical'.	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' deasserted 'below lower critical'.
External Sensor Slot > * > State Sensor > Unavailable	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' unavailable.	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' available.
External Sensor Slot > * > State Sensor > Closed	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is closed.	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is open.
External Sensor Slot > * > State Sensor > On	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is on.	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is off.
External Sensor Slot > * > State Sensor > Alarmed	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is alarmed.	External sensor '[EXTSENSORNAME]' in slot '[EXTSENSORSLOT]' is no longer alarmed.
Server Monitoring > * > Monitored	Server '[SERVER]' is now being monitored.	Server '[SERVER]' is no longer being monitored.
Server Monitoring > * > Unreachable	Server '[SERVER]' is unreachable.	Server '[SERVER]' is reachable.
EnergyWise > Enabled	User '[USERNAME]' from host '[USERIP]' enabled EnergyWise.	User '[USERNAME]' from host '[USERIP]' disabled EnergyWise.
Asset Management > State	State of asset strip [STRIPID] ('[STRIPNAME]') changed to '[STATE]'.	
Asset Management > Rack Unit > * > Tag Connected	Asset tag with ID '[TAGID]' connected at rack unit [RACKUNIT], slot [RACKSLOT] of asset strip [STRIPID] ('[STRIPNAME]').	Asset tag with ID '[TAGID]' disconnected at rack unit [RACKUNIT], slot [RACKSLOT] of asset strip [STRIPID] ('[STRIPNAME]').
Asset Management > Rack Unit > * > Blade Extension Connected	Blade extension with ID '[TAGID]' connected at rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]').	Blade extension with ID '[TAGID]' disconnected at rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]').
Asset Management > Firmware Update	Firmware update for asset strip [STRIPID] ('[STRIPNAME]'): status changed to '[STATE]'.	

Asset Management > Device Config Changed	Config parameter '[PARAMETER]' of asset strip [STRIPID] ('[STRIPNAME]') changed to '[VALUE]' by user '[USERNAME]'.	
Asset Management > Rack Unit Config Changed	Config of rack unit [RACKUNIT] of asset strip [STRIPID] ('[STRIPNAME]') changed by user '[USERNAME]' to: LED Operation Mode '[LEDOPMODE]', LED Color '[LEDCOLOR]', LED Mode '[LEDMODE]'	
Asset Management > Blade Extension Overflow	Blade extension overflow occurred on strip [STRIPID] ('[STRIPNAME]').	Blade extension overflow cleared for strip [STRIPID] ('[STRIPNAME]').
Asset Management > Composite Asset Strip Composition Changed	Composition changed on composite asset strip [STRIPID] ('[STRIPNAME]').	
RF Code Tag > Connected	RF Code tag has been connected.	RF Code tag has been disconnected.
LHX > Connected	LHX has been connected to [PORTTYPE] port [PORTID].	LHX has been disconnected from [PORTTYPE] port [PORTID].
LHX > Operational State	LHX connected to [PORTTYPE] port [PORTID] has been switched on.	LHX connected to [PORTTYPE] port [PORTID] has been switched off.
LHX > Sensor > Unavailable	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' unavailable.	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' available.
LHX > Sensor > Above upper critical threshold	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'above upper critical'.	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'above upper critical'.
LHX > Sensor > Above upper warning threshold	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'above upper warning'.	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'above upper warning'.
LHX > Sensor > Below lower warning threshold	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'below lower warning'.	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'below lower warning'.
LHX > Sensor > Below lower critical threshold	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' asserted 'below lower critical'.	Sensor '[LHXSENSORID]' on LHX at [PORTTYPE] port '[PORTID]' deasserted 'below lower critical'.
LHX > Emergency Cooling	Emergency cooling on LHX at [PORTTYPE] port '[PORTID]' was activated.	Emergency cooling on LHX at [PORTTYPE] port '[PORTID]' was deactivated.

LHX > Maximum cooling request	Maximum cooling was requested for LHX at [PORTTYPE] port '[PORTID]'.	Maximum cooling is not any more requested for LHX at [PORTTYPE] port '[PORTID]'.
LHX > Parameter Data Loss	Data loss in parameter memory was detected on LHX at [PORTTYPE] port '[PORTID]'.	
LHX > ST-Bus Communication Error	An ST-Bus communication error was detected on LHX at [PORTTYPE] port '[PORTID]'.	
LHX > Collective fault	A collective fault occurred on LHX at [PORTTYPE] port '[PORTID]'.	
LHX > Door Contact	The door of LHX at [PORTTYPE] port '[PORTID]' was opened.	The door of LHX at [PORTTYPE] port '[PORTID]' was closed.
LHX > Sensor Failure	A sensor failure (broken or short circuit) occurred on LHX at [PORTTYPE] port '[PORTID]' at sensor '[LHXSENSORID]'.	
LHX > Fan Failure	A fan motor failure occurred on LHX at [PORTTYPE] port '[PORTID]' at fan '[LHXFANID]'.	
LHX > Power Supply Failure	A power supply failure occurred on LHX at [PORTTYPE] port '[PORTID]' at power supply '[LHXPOWERSUPPLYID]'.	
LHX > Threshold Air Inlet	The air inlet temperature threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed.	The air inlet temperature on LHX at [PORTTYPE] port '[PORTID]' is within thresholds.
LHX > Threshold Air Outlet	The air outlet temperature threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed.	The air outlet temperature on LHX at [PORTTYPE] port '[PORTID]' is within thresholds.
LHX > Threshold Water Inlet	The water inlet temperature threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed.	The water inlet temperature on LHX at [PORTTYPE] port '[PORTID]' is within thresholds.
LHX > Threshold Water Outlet	The water outlet temperature threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed.	The water outlet temperature on LHX at [PORTTYPE] port '[PORTID]' is within thresholds.
LHX > Threshold Humidity	The humidity threshold on LHX at [PORTTYPE] port '[PORTID]' was crossed.	The humidity on LHX at [PORTTYPE] port '[PORTID]' is within thresholds.
LHX > External Water Cooling Failure	An external water cooling failure occurred on LHX at [PORTTYPE] port '[PORTID]'.	

LHX > Water Leak	Water leakage was detected on LHX at [PORTTYPE] port '[PORTID]'.	

**Note: Not set for 'trigger' events.*

Email and SMS Message Placeholders

Following are placeholders that can be used in custom event email messages.

Note: Click the Information icon to open the Event Context Information dialog, which contains a list of placeholders and their definitions. Then select the desired placeholder, and either double-click it or click the "Paste into message" button to insert it into the customized message.

Placeholder	Definition
[ACTIVEINLET]	The label of the newly activated inlet
[AMSBLADESLOTPOSITION]	The (horizontal) slot position, an action applies to
[AMSLEDCOLOR]	The RGB LED color
[AMSLEDMODE]	The LED indication mode
[AMSLEDOPMODE]	The LED operating mode
[AMSNAME]	The name of an asset strip
[AMSNUMBER]	The numeric ID of an asset strip
[AMSRACKUNITPOSITION]	The (vertical) rack unit position, an action applies to
[AMSSTATE]	The human readable state of an asset strip
[AMSTAGID]	The asset tag ID
[CONFIGPARAM]	The name of a configuration parameter
[CONFIGVALUE]	The new value of a configuration parameter
[DATETIME]	The human readable timestamp of the event occurrence
[DEVICEIP]	The IP address of the device, the event occurred on
[DEVICENAME]	The name of the device, the event occurred on
[EXTSENSORNAME]	The name of an external sensor
[EXTSENSORSLOT]	The ID of an external sensor slot
[IFNAME]	The human readable name of a network interface
[INLETPOLE]	The inlet power line identifier
[INLETSENSOR]	The inlet sensor name

Placeholder	Definition
[INLET]	The power inlet label
[ISASSERTED]	Boolean flag whether an event condition was entered (1) or left (0)
[LDAPERRORDESC]	An LDAP error occurred
[LHXFANID]	The ID of a fan connected to an LHX
[LHXPOWERSUPPLYID]	The ID of an LHX power supply
[LHXSENSORID]	The ID of an LHX sensor probe
[LEDCOLOR]	The RGB LED color
[LEDMODE]	The LED indication mode
[LEDOPMODE]	The LED operating mode
[MONITOREDHOST]	The name or IP address of a monitored host
[OCPSENSOR]	The overcurrent protector sensor name
[OCP]	The overcurrent protector label
[OLDVERSION]	The firmware version the device is being upgraded from
[OUTLETPOLE]	The outlet power line identifier
[OUTLETSENSOR]	The outlet sensor name
[OUTLET]	The outlet label
[PDUPOLESENSOR]	The sensor name for a certain power line
[PORTID]	The label of the external port, the event triggering device is connected to
[PORTTYPE]	The type of the external port (for example, 'feature' or 'auxiliary'), the event triggering device is connected to
[SENSORREADINGUNIT]	The unit of a sensor reading
[SENSORREADING]	The value of a sensor reading
[SMTPRECIPIENTS]	The list of recipients, an SMTP message was sent to
[SMTPSERVER]	The name or IP address of a server
[TIMESTAMP]	The timestamp of the event occurrence
[TRANSFERSWITCHREASON]	The transfer reason (automatic or manual)
[TRANSFERSWITCHSENSOR]	The transfer switch sensor name
[TRANSFERSWITCH]	The transfer switch label
[UMTARGETROLE]	The name of a user management role, an action was applied on

Placeholder	Definition
[UMTARGETUSER]	The user, an action was triggered for
[USERIP]	The IP address, a user connected from
[USERNAME]	The user who triggered an action
[VERSION]	The firmware version the device is upgrading to
[WIRESENSOR]	The wire sensor name
[WIRE]	The wire label

Sample Event Rules

Sample PDU-Level Event Rule

In this example, we want the PX to record the firmware upgrade failure in the internal log when it happens. The sample event rule looks like this:

- Event: Device > Firmware update failed
- Actions: System Event Log Action

To create the above event rule:

1. Select Event > Device to indicate we are specifying an event at the PDU level.
2. Select "Firmware update failed" in the submenu because we want PX to respond to the event related to firmware upgrade failure.
3. Select System Event Log Action as we intend to record the firmware update failure event in the internal log.

Sample Outlet-Level Event Rule

In this example, we want the PX to send SNMP notifications to the SNMP manager for any sensor change event of outlet 3.

Note: The SNMP notifications may be SNMP v2c or SNMP v3 traps or informs, depending on the settings for the System SNMP Notification Action. See **Configuring SNMP Notifications** *(on page 265).*

To do that we would set up an event rule like this:

- Event: Outlet > Outlet 3 > Sensor > Any sub-event
- Actions: System SNMP Notification Action

To create the above event rule:

1. Select Event > Outlet to indicate we are specifying an event at the outlet level.

2. Select "Outlet 3" from the submenu because that is the outlet in question.
3. Select "Sensor" to refer to sensor events.
4. Select "Any sub-event" because we want to specify all events related to all types of outlet sensors and thresholds, such as current, voltage, upper critical threshold, upper warning threshold, lower critical threshold, lower warning threshold, and so on.
5. Select "System SNMP Notification Action" to send SNMP notifications to respond to the specified event.

   Then the SNMP notifications are sent when:

   - Any numeric sensor reading moves past any threshold into the warning or critical range.
   - Any sensor reading or state returns to normal.
   - Any sensor becomes unavailable.
   - Any discrete sensor changes its state -- either from normal to alarmed or from alarmed to normal.

   For example, when the outlet 3's voltage crosses into the upper warning range, the SNMP notifications are sent, and when the voltage drops below the upper warning threshold, the SNMP notifications are sent again.

Sample Inlet-Level Event Rule

In this example, we want the PX to send SNMP notifications to the SNMP manager for any sensor change event of the Inlet I1.

Note: The SNMP notifications may be SNMP v2c or SNMP v3 traps or informs, depending on the settings for the System SNMP Notification Action. See **Configuring SNMP Notifications** *(on page 265).*

The event rule is set like this:

- Event: Inlet > Inlet I1 > Sensor > Any sub-event
- Actions: System SNMP Notification Action

To create the above event rule:

1. Select Event > Inlet to indicate we are specifying an event at the inlet level.
2. Select "Inlet I1" from the submenu because that is the inlet in question.
3. Select "Sensor" to refer to sensor events.
4. Select "Any sub-event" because we want to specify all events related to all types of inlet sensors and thresholds, such as current, voltage, upper critical threshold, upper warning threshold, lower critical threshold, lower warning threshold, and so on.

5. Select "System SNMP Notification Action" to send SNMP notifications to respond to the specified event.

   Then the SNMP notifications are sent when:

   - Any numeric sensor reading moves past any threshold into the warning or critical range.
   - Any sensor reading or state returns to normal.
   - Any sensor becomes unavailable.

   For example, when the Inlet I1's voltage crosses into the upper warning range, the SNMP notifications are sent, and when the voltage drops below the upper warning threshold, the SNMP notifications are sent again.

Sample Environmental-Sensor-Level Event Rule

This section only applies to outlet-switching capable PDUs.

In this example, we want PX to enable the load shedding function when a contact closure sensor enters the alarmed state. This sample event rule requires the creation of a new action before creating the rule.

Step 1: create a new action for enabling the load shedding mode

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. Click the Actions tab.
3. Click New Action.
4. In the Action Name field, type a name to identify this action. In this illustration, type Enable Load Shedding.
5. In the Action field, select "Change load shedding state."
6. In the Operation field, select "Enable load shedding."
7. Click Save to save this action.

After the new action for enabling the load shedding mode is created, you can create an event rule that can trigger the load shedding mode when the contact closure sensor enters the alarmed state. This sample event rule looks like this:

- Event: External Sensor Slot > Slot 1 > State Sensor > Alarmed
- Trigger condition: Alarmed
- Actions: Enable Load Shedding

Step 2: create the contact closure triggered load shedding event rule

1. Click the Rules tab.
2. Click New Rule.
3. In the "Rule name" field, type a name to identify this event rule. In this illustration, type Contact Closure Triggered Load Shedding.
4. Select the Enabled checkbox. Otherwise, the new event rule will not be carried out.
5. Select Events > External Sensor Slot to indicate we are specifying an event related to the environmental sensor.
6. Select the ID number of the desired contact closure sensor. In this illustration, the ID number of the desired contact closure sensor is 1, so select Slot 1 in the submenu.
7. Select State Sensor because the contact closure sensor is a discrete sensor, which indicates the environmental changes through the status changes.
8. Select Alarmed in the submenu since we want the action "Enable Loading Shedding" to be taken when the selected contact closure sensor changes its state related to the "alarmed" state.
9. In the "Trigger condition" field, select the Alarmed radio button because we want the PX to respond to the event only when the contact closure sensor enters the Alarm state.

A Note about Infinite Loop

You should avoid building an infinite loop when creating event rules.

The infinite loop refers to a condition where the PDU keeps busy because the action or one of the actions taken for a certain event triggers an identical or similar event which will result in an action triggering one event again.

Example 1

This example illustrates an event rule which continuously causes the PDU to send out SMTP messages.

Event selected	Action included
Device > Sending SMTP message failed	Send SMTP message

Example 2

This example illustrates an event rule which continuously causes the PDU to send out SMTP messages when one of the selected events listed on the Device menu occurs. Note that the <Any sub-event> under the Device menu includes the event "Sending SMTP message failed."

Event selected	Action included
Device > Any sub-event	Send SMTP message

Example 3

This example illustrates a situation where two event rules combined regarding the outlet state changes causes the PDU to continuously power cycle outlets 1 and 2.

Event selected	Action included
Outlet > Outlet 1 > Sensor > State > On/Off	Cycle Outlet 2 (Switch Outlets --> Cycle Outlet --> Outlet 2)
Outlet > Outlet 2 > Sensor > State > On/Off	Cycle Outlet 1 (Switch Outlets --> Cycle Outlet --> Outlet 1)

Modifying an Event Rule

You can change an event rule's event, action, trigger condition and other settings, if any.

Exception: Events and actions selected in the built-in event rules are not changeable, including System Event Log Rule and System SNMP Notification Rule.

To modify an event rule:

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. On the Rules tab, select the event rule that you want to modify in the left pane.
3. To disable the event rule, deselect the Enabled checkbox.
4. To change the event, click the desired tab in the Event field and select a different item from the pull-down menu or submenu.

   For example, in a user activity event rule for the "admin" user, you can click the "admin" tab to display a pull-down submenu showing all user names, and then select a different user name or all user names (referred to as <*Any user*>).
5. If radio buttons are available, you may select a radio button other than the current selection to change the rule triggering condition.
6. To change the action(s), do any of the following in the Actions field:
   - To add any action, select it from the "Available actions" list box, and click the Add button . To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
   - To add all actions at a time, click the Add All button .
   - To remove any action, select it from the "Selected actions" list box, and click the Remove button to move it back to the "Available actions" list box. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
   - To remove all actions at a time, simply click the Remove All button .
   - To create a new action, click Create New Action. The newly created action will be moved into the "Selected actions" list box once it is created. See ***Creating Actions*** (on page 181) for information on creating an action.
7. Click Save to save the changes.

Note: If you do not click Save before quitting the current settings page, a message appears. Then click Yes to save the changes, Discard to abort or Cancel to return to the current settings page.

8. Click Close to quit the dialog.

Modifying an Action

An existing action can be changed so that all event rules where this action is involved change their behavior accordingly.

Exception: The built-in action "System Event Log Action" is not user-configurable.

To modify an action:

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. Click the Actions tab.
3. Select the action that you want to modify from the left list.
4. Make necessary changes to the information shown.
5. Click Save to save the changes.

   Note: If you do not click Save before quitting the current settings page, a message appears. Then click Yes to save the changes, Discard to abort or Cancel to return to the current settings page.

6. Click Close to quit the dialog.

Deleting an Event Rule or Action

If any event rule or action is obsolete, simply remove it.

Note: You cannot delete the built-in event rules and actions.

To delete an event rule or action:

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. To delete an event rule:
   a. Ensure the Rules tab is selected. If not, click the Rules tab.
   b. Select the desired rule from the left list, and click Delete Rule.
   c. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.
3. To delete an action:
   a. Click the Actions tab.
   b. Select the desired action from the left list, and click Delete Action.
   c. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.

4. Click Close to quit the dialog.

A Note about Untriggered Rules

In some cases, a measurement exceeds a threshold causing the PX to generate an alert. The measurement then returns to a value within the threshold, but the PX does not generate an alert message for the Deassertion event. Such scenarios can occur due to the hysteresis tracking the PX uses. See ***What is Deassertion Hysteresis?*** (on page 178).

Managing Event Logging

By default, the PX captures certain system events and saves them in a local (internal) event log.

Viewing the Local Event Log

You can view up to 2,000 historical events that occurred to the PX device in the local event log.

When the log already contains 2,000 entries, each new entry overwrites the oldest entry.

To display the local log:

1. Choose Maintenance > View Event Log. The Event Log dialog appears.

   Each event entry in the local log consists of:

   - Date and time of the event
   - Type of the event
   - A description of the event
   - ID number of the event

2. The dialog shows the final page by default. You can:

   - Switch between different pages by doing one of the following:

     - Click or to go to the first or final page.

     - Click or to go to the prior or next page.

     - Type a number in the Page text box and press Enter to go to a specific page.

   - Select a log entry from the list and click Show Details, or simply double-click the log entry to view detailed information.

Note: Sometimes when the dialog is too narrow, the icon » takes the place of the Show Details button. In that case, click » and select Show Details to view details.

- Click ⏭ to view the latest events.
- View only a specific type of events by selecting an event class in the Filter Event Class field.

Clearing Event Entries

If it is not necessary to keep existing event history, you can remove all of it from the local log.

To delete all event entries:

1. Choose Maintenance > View Event Log. The Event Log dialog appears.
2. Click Clear Event Log.
3. Click Yes on the confirmation message.

Viewing Connected Users

You can see which users are connected to the PX device and their status. If you have administrator privileges, you can terminate any user's connection to the PX device.

To view connected users:

1. Choose Maintenance > Connected Users. The Connected Users dialog appears, showing a list of connected users with the following information:

Column	Description
User Name	The login name used by each connected user.
IP Address	The IP address of each user's host. For the login via a local connection (serial or USB), <local> is displayed instead of an IP address.
Client Type	The interface through which the user is being connected to the PX. ▪ Web GUI: Refers to the PX web interface. ▪ CLI: Refers to the command line interface (CLI). The information in parentheses following "CLI" indicates how this user was connected to the CLI. - *Serial*: Represents the local connection (serial or USB). - *SSH*: Represents the SSH connection. - *Telnet*: Represents the Telnet connection.

Column	Description
Idle Time	The length of time for which a user remains idle. The unit "min" represents minutes.

2. To disconnect any user, click the corresponding Disconnect button.
   a. A dialog appears, prompting you to confirm the operation.
   b. Click Yes to disconnect the user or No to abort the operation. If clicking Yes, the connected user is forced to log out.
3. You may change the sorting order of the list if necessary. See ***Changing the Sorting*** (on page 91).
4. Click Close to quit the dialog.

Monitoring Server Accessibility

You can monitor whether specific IT devices are alive by having the PX device continuously ping them. An IT device's successful response to the ping commands indicates that the IT device is still alive and can be remotely accessed.

Adding IT Devices for Ping Monitoring

You can have the PX monitor the accessibility of any IT equipment, such as DB servers, remote authentication servers or any power distribution unit (PDU). The PX supports monitoring a maximum of 8 devices.

The default ping settings may not be suitable for monitoring devices that require high connection reliability so it is strongly recommended that you should adjust the ping settings to meet your own needs.

Tip: To make the PX automatically log, send notifications or perform other actions for any server accessibility or inaccessibility events, you can create event rules associated with server monitoring. See **Event Rules and Actions** *(on page 180).*

To add IT equipment for ping monitoring:

1. Choose Device Settings > Server Reachability. The Server Reachability dialog appears.
2. Click New. The Add New Server dialog appears.
3. By default, the "Enable Ping Monitoring for this Server" checkbox is selected. If not, select it to enable the ping monitoring feature.
4. Provide the information required.

Field	Description
IP Address/Hostname	IP address or host name of the IT equipment whose accessibility you want to monitor.
Number of Successful Pings to Enable Feature	The number of successful pings required to declare that the monitored equipment is "Reachable." Valid range is 0 to 200.
Wait Time (in seconds) after Successful Ping	The wait time before sending the next ping if the previous ping was successfully responded. Valid range is 5 to 600 (seconds).
Wait Time (in seconds) after Unsuccessful Ping	The wait time before sending the next ping if the previous ping was not responded. Valid range is 3 to 600 (seconds).
Number of Consecutive Unsuccessful Pings for Failure	The number of consecutive pings without any response before the monitored equipment is declared "Unreachable." Valid range is 1 to 100.
Wait Time (in seconds) before Resuming Pinging	The wait time before the PX resumes pinging after the monitored equipment is declared unreachable. Valid range is 1 to 1200 (seconds).

5. Click OK to save the changes.
6. To add more IT devices, repeat Steps 2 to 5.
7. Click Close to quit the dialog.

In the beginning, the status of the monitored equipment shows "Waiting for reliable connection," which means the requested number of consecutive successful or unsuccessful pings has not reached before the PX can declare that the monitored device is reachable or unreachable.

Example: Ping Monitoring and SNMP Notifications

In this illustration, it is assumed that a significant PDU (IP address: 192.168.84.95) shall be monitored by your PX to make sure that PDU is properly operating all the time, and the PX must send out SNMP notifications (trap or inform) if that PDU is declared unreachable due to power or network failure. The prerequisite for this example is that the power source for your PX is different from the power source for that PDU.

This requires two steps: set up the PDU monitoring and create an event rule.

Step 1: Set up the ping monitoring for the target PDU

1. Choose Device Settings > Server Reachability. The Server Reachability dialog appears.
2. Type 192.168.84.95 in the IP Address/Hostname field.
3. To make the PX declare the accessibility of the monitored PDU every 15 seconds (3 pings * 5 seconds) when that PDU is accessible, do the following:
   a. In the Number of Successful Pings to Enable Feature field, type 3.
   b. In the Wait Time (in seconds) after Successful Ping field, type 5.
4. To make the PX declare the inaccessibility of the monitored PDU when that PDU becomes inaccessible for around 12 seconds (4 pings * 3 seconds), do the following:
   a. In the Number of Consecutive Unsuccessful Pings for Failure field, type 4.
   b. In the Wait Time (in seconds) after Unsuccessful Ping field, type 3.
5. In the Wait Time (in seconds) before Resuming Pinging field, type 60 to make the PX stops pinging the target PDU for 60 seconds (1 minute) after the PDU inaccessibility is declared. After 60 seconds, the PX will re-ping the target PDU.

Step 2: Create an event rule to send SNMP notifications for this PDU

1. Choose Device Settings > Event Rules. The Event Rule Settings dialog appears.
2. Click New.
3. In the "Rule name" field, type "Send SNMP notifications for PDU (192.168.84.95) inaccessibility."
4. Select the Enabled checkbox to enable this new rule.
5. In the Event field, choose Server Monitoring > 192.168.84.95 > Unreachable.

6. In the "Trigger condition" field, select the Unreachable radio button. This makes the PX react only when the target PDU becomes inaccessible.
7. Select the System SNMP Notification Action from the "Available actions" list box, and click to add it to the "Selected actions" list box.

Note: If you have not configured the System SNMP Notification Action to specify the SNMP destination(s), see **Configuring SNMP Notifications** *(on page 265).*

Editing Ping Monitoring Settings

You can edit the ping monitoring settings for any IT device whenever it requires changes.

To modify the ping monitoring settings for an IT device:

1. Choose Device Settings > Server Reachability. The Server Reachability dialog appears.
2. Select the IT device whose settings you want to modify by clicking it.
3. Click Edit or double-click the IT device. The Edit Server 'XXX' dialog appears, where XXX is the IP address or host name of the IT device.
4. Make changes to the information shown.
5. Click OK to save the changes.

Deleting Ping Monitoring Settings

When it is not necessary to monitor the accessibility of any IT device, just remove it.

To delete ping monitoring settings for an IT device:

1. Choose Device Settings > Server Reachability. The Server Reachability dialog appears.
2. Select the IT device whose ping monitoring settings you want to remove by clicking it. To make multiple selections, press Ctrl+click or Shift+click to highlight multiple ones.
3. Click Delete.
4. A message appears, prompting you to confirm the operation. Click Yes to confirm the deletion.
5. Click Close to quit the dialog.

Checking Server Monitoring States

Server monitoring results are available in the Server Reachability dialog after specifying servers for the PX device to monitor.

To check the server monitoring states and results:

1. Choose Device Settings > Server Reachability. The Server Reachability dialog appears.
2. The column labeled "Ping Enabled" indicates whether the monitoring for the corresponding server is activated or not.
   - : This icon denotes that the monitoring for the corresponding server is enabled.
   - : This icon denotes that the monitoring for the corresponding server is disabled.
3. The column labeled "Status" indicates the accessibility of each monitored server.

Status	Description
Reachable	The server is accessible.
Unreachable	The server is inaccessible.
Waiting for reliable connection	The connection between the PX device and the server is not established yet.

4. You may change the sorting order of the list if necessary. See ***Changing the Sorting*** (on page 91).
5. Click Close to quit the dialog.

Environmental Sensors

The PX can monitor the environmental conditions, such as temperature and humidity, where environmental sensors are placed.

To add environmental sensors:

1. Physically connect environmental sensors to the PX device. See ***Connecting Environmental Sensors (Optional)*** (on page 33).
2. Log in to the PX web interface. The PX should have detected the connected sensors, and display them in the web interface.
3. Identify each sensor through the sensor's serial number. See ***Identifying Environmental Sensors*** (on page 222).
4. The PX should automatically manage the detected sensors. Verify whether detected sensors are managed. If not, have them managed. See ***Managing Environmental Sensors*** (on page 223).

5. Configure the sensors. See ***Configuring Environmental Sensors*** (on page 224). The steps include:
   a. Name the sensor.
   b. If the connected sensor is a Raritan contact closure sensor, specify an appropriate sensor type.
   c. Mark the sensor's physical location on the rack or in the room.
   d. For a numeric sensor, configure the sensor's threshold, hysteresis and assertion timeout settings.
   e. For a numeric sensor, configure the sensor's threshold, hysteresis and assertion timeout settings.

Note: Numeric sensors use numeric values to indicate the environmental or internal conditions while discrete (on/off) sensors use alphabetical characters only to indicate the state changes. Only numeric sensors have the threshold settings.

Identifying Environmental Sensors

An environmental sensor includes a serial number tag on the sensor cable.

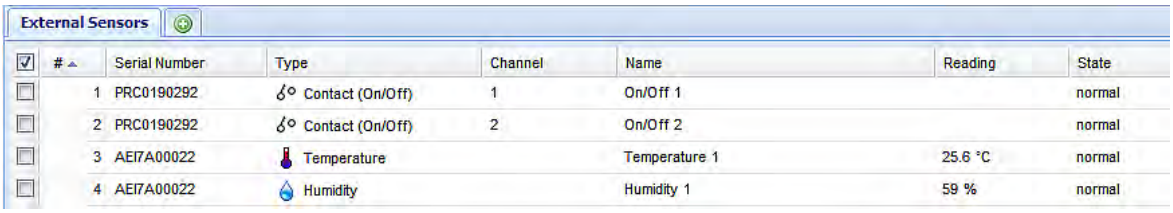
The serial number for each sensor appears listed in the web interface after each sensor is detected by the PX.

To identify each detected environmental sensor:

1. If the PDU folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 83).

   Note: The PDU folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the PDU** *(on page 98).*

2. Click External Sensors in the Dominion PX Explorer pane, and the External Sensors page opens in the right pane.



#	Serial Number	Type	Channel	Name	Reading	State
1	PRC0190292	Contact (On/Off)	1	On/Off 1		normal
2	PRC0190292	Contact (On/Off)	2	On/Off 2		normal
3	AEI7A00022	Temperature		Temperature 1	25.6 °C	normal
4	AEI7A00022	Humidity		Humidity 1	59 %	normal

3. Match the serial number from the tag to those listed in the sensor table.

Managing Environmental Sensors

The PX starts to retrieve an environmental sensor's reading and/or state and records the state transitions after the environmental sensor is managed.

The PX device can manage a maximum of 16 environmental sensors.

When there are less than 16 managed sensors, the PX automatically brings detected environmental sensors under management. You should only have to manually manage a sensor when it is not under management.

To manually manage an environmental sensor:

1. If the PDU folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 83).

   Note: The PDU folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the PDU** *(on page 98).*

   ---

2. Click External Sensors in the Dominion PX Explorer pane, and the External Sensors page opens in the right pane.
3. Select the checkbox of the sensor you want to manage on the External Sensors page. To manage multiple sensors, select the checkboxes of all desired sensors.

   Note: To identify all detected sensors, see **Identifying Environmental Sensors** *(on page 222).*

   ---

4. Click Manage. If you selected only one sensor, the "Manage sensor <serial number> (<sensor type>)" dialog appears, where <serial number> is the sensor's serial number and <sensor type> is the sensor's type.

   Note: For a contact closure sensor, a channel number is added to the end of the <sensor type>.

   ---

5. There are two ways to manage the sensor:

- To manage this sensor by letting the PX assign a number to it, select "Automatically assign a sensor number." This method does not release any managed sensors.
- To manage this sensor by assigning the number you want to it, select "Manually select a sensor number." Then click the drop-down arrow to select a number.

  If the number you selected was already assigned to a sensor, that sensor becomes released after losing this ID number.

Tip: The information in parentheses following each ID number indicates whether the number has been assigned to any sensor. If it has been assigned to a sensor, it shows that sensor's serial number. Otherwise, it shows the term "unused."

The manual assignment method is unavailable if you selected multiple sensors in Step 1.

6. Click OK. The PX starts to track and display the managed sensor's reading and/or state.
7. To manage additional sensors, repeat Steps 3 to 6.

Note: When the number of managed sensors reaches the maximum, you CANNOT manage additional sensors until you remove or replace any managed sensors. To remove a sensor, see **Unmanaging Environmental Sensors** *(on page 232).*

Configuring Environmental Sensors

You may change the default name for easily identifying the managed sensor, and describe its location with X, Y and Z coordinates.

To configure environmental sensors:

1. If the PDU folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 83).

   Note: The PDU folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the PDU** *(on page 98).*

2. Click External Sensors in the Dominion PX Explorer pane, and the External Sensors page opens in the right pane.
3. Select the sensor that you want to configure.
4. Click Setup. The "Setup of external sensor <serial number> (<sensor type>)" dialog appears, where <serial number> is the serial number of this sensor and <sensor type> is the sensor's type.

Tip: You can also trigger the same setup dialog by selecting the desired environmental sensor icon in the tree and then clicking Setup on that sensor's page opened in the right pane.

5. If the selected environmental sensor is the Raritan contact closure sensor connected with a third-party detector/switch, select the appropriate sensor type in the Binary Sensor Subtype field.
   - Contact: The detector/switch is designed to detect the door lock or door open/closed status.
   - Smoke Detection: The detector/switch is designed to detect the appearance of smoke.
   - Water Detection: The detector/switch is designed to detect the appearance of water on the floor.
   - Vibration: The detector/switch is designed to detect the vibration in the floor.
6. Type a new name in the Name field.
7. Describe the sensor's location by assigning alphanumeric values to the X, Y and Z coordinates. See ***Describing the Sensor Location*** (on page 227).

Note: When the term "Rack Units" appears inside the parentheses in the Z location field, indicating that the Z coordinate format is set to Rack Units, you must type an integer number.

8. If the selected environmental sensor is a numeric sensor, its threshold settings are displayed in the dialog. Click Edit or double-click the Threshold Configuration table to adjust the threshold, deassertion hysteresis and assertion timeout settings.
   - To enable any threshold, select the corresponding checkbox. To disable a threshold, deselect the checkbox.
   - After any threshold is enabled, type an appropriate numeric value in the accompanying text box.
   - To enable the deassertion hysteresis for all thresholds, type a numeric value other than zero in the Deassertion Hysteresis field. See ***What is Deassertion Hysteresis?*** (on page 178).
   - To enable the assertion timeout for all thresholds, type a numeric value other than zero in the Assertion Timeout (samples) field. See ***What is Assertion Timeout?*** (on page 179).

Note: The Upper Critical and Lower Critical values are points at which the PX considers the operating environment critical and outside the range of the acceptable threshold.

9. Click OK to save the changes.
10. Repeat Steps 3 through 9 to configure additional environmental sensors.

Setting the Z Coordinate Format

You can use either the number of rack units or a descriptive text to describe the vertical locations (Z coordinates) of environmental sensors.

To determine the Z coordinate format:

1. Click the PDU folder.

   Note: The PDU folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the PDU** *(on page 98).*

2. Click Setup in the Settings section. The Pdu Setup dialog appears.
3. In the "External sensors Z coordinate format" field, click the drop-down arrow and select an option from the list.
   - Rack Units: The height of the Z coordinate is measured in standard rack units. When this is selected, you can type a numeric value in the rack unit to describe the Z coordinate of any environmental sensors.
   - Free-Form: Any alphanumeric string can be used for specifying the Z coordinate.
4. Click OK to save the changes.

Describing the Sensor Location

Use the X, Y and Z coordinates to describe each sensor's physical location. You can use these location values to track records of environmental conditions in fixed locations around your IT equipment. The X, Y and Z values act as additional attributes and are not tied to any specific measurement scheme. If you choose to, you can use non-measurement values. For example:

X = *Brown Cabinet Row*

Y = *Third Rack*

Z = *Top of Cabinet*

Values for the X, Y and Z coordinates may consist of:

- For X and Y: Any combination of alphanumeric characters. The coordinate value can be 0 to 32 characters long.
- For Z when the Z coordinate format is set to *Rack Units*, any numeric value ranging from 0 to 60.
- For Z when the Z coordinate format is set to *Free-Form*, any alphanumeric characters from 0 to 32 characters.

Tip: To configure and retrieve these coordinate values over SNMP, see the PX MIB. To configure and retrieve these values over the CLI, see **Using the Command Line Interface** *(on page 273).*

Setting Thresholds for Multiple Sensors

You can configure thresholds for multiple environmental sensors of *the same type* at a time. For example, if you want all temperature sensors to have identical upper and lower thresholds, follow the procedure below to set up all temperature sensors together.

To configure thresholds of multiple environmental sensors:

1. Click External Sensors in the Dominion PX Explorer pane, and the External Sensors page opens in the right pane.
2. Select the checkboxes of those environmental sensors whose threshold settings should be the same. Make sure the selected sensors belong to the same type.
   - To select all environmental sensors listed on the External Sensors page, have the checkbox in the header row selected.
3. Click Setup. Note that the Setup button is disabled if any of the selected sensors belongs to a different type.
4. Configure the thresholds as described in ***Configuring Environmental Sensors*** (on page 224).

Viewing Sensor Data

Readings of the environmental sensors will display in the web interface after these sensors are properly connected and managed.

The Dashboard page shows the information for managed environmental sensors only, while the External Sensors page shows the information for both of managed and unmanaged ones.

If a sensor reading row is colored, it means the sensor reading already crosses one of the thresholds, or the circuit breaker has tripped. See ***The Yellow- or Red-Highlighted Reading*** (on page 89).

To view managed environmental sensors only:

1. Click the Dashboard icon in the Dominion PX Explorer pane, and the Dashboard page opens in the right pane.
2. Locate the External Sensors section on the Dashboard page. The section shows:
   - Total number of managed sensors
   - Total number of unmanaged sensors
   - Information of each managed sensor, including:
     - Name
     - Reading
     - State

To view both of managed and unmanaged environmental sensors:

1. If the PDU folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 83).

   Note: The PDU folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the PDU** *(on page 98).*

2. Click External Sensors in the Dominion PX Explorer pane, and the External Sensors page opens in the right pane.

   Detailed information for each connected sensor is displayed, including:
   - Label (number)
   - Serial number
   - Sensor type
   - Name
   - Reading

- State
- Channel (for a contact closure sensor only)

Sensor Measurement Accuracy

Raritan environmental sensors are with the following factory specifications. Calibration is not required for environmental sensors.

- Temperature: +/-2 degrees Celsius
- Humidity: +/-5% (when humidity < 60%) or +/-8% (when humidity > 60%)
- Differential air pressure: +/-1.5%
- Air flow: +/-6.5%

States of Managed Sensors

An environmental sensor shows the state after being managed.

Available sensor states vary depending on the sensor type -- numeric or discrete sensors. For example, a contact closure sensor is a discrete (on/off) sensor so it switches between three states only -- unavailable, alarmed and normal.

Note: Numeric sensors use numeric values to indicate the environmental or internal conditions while discrete (on/off) sensors use alphabetical characters only to indicate the state changes.

Sensor state	Applicable to
unavailable	All sensors
alarmed	Discrete sensors
normal	All sensors
below lower critical	Numeric sensors
below lower warning	Numeric sensors
above upper warning	Numeric sensors
above upper critical	Numeric sensors

"unavailable" State

The *unavailable* state means the connectivity to the sensor is lost.

The Raritan PX pings all managed sensors at regular intervals in seconds. If it does not detect a particular sensor for three consecutive scans, the *unavailable* state is displayed for that sensor.

When the communication with a contact closure sensor's processor is lost, all detectors (that is, all switches) connected to the same sensor module show the "unavailable" state.

Note: When the sensor is deemed unavailable, the existing sensor configuration remains unchanged. For example, the ID number assigned to the sensor remains associated with it.

The Raritan PX continues to ping unavailable sensors, and moves out of the *unavailable* state after detecting the sensor for two consecutive scans.

"normal" State

This state indicates the sensor is in the normal state.

For a contact closure sensor, usually this state is the normal state you have set.

- If the normal state is set to Normally Closed, the *normal* state means the contact closure switch is closed.
- If the normal state is set to Normally Open, the *normal* state means the contact closure switch is open.

For a Raritan's floor water sensor, the normal state must be set to Normally Closed, which means no water is detected.

Note: See **Configuring a Contact Closure Sensor** *(on page 41) for information on setting the normal state or dip switch.*

For a numeric sensor, this state means the sensor reading is within the acceptable range as indicated below:

Lower Warning threshold <= Reading < Upper Warning threshold

Note: The symbol <= means smaller than (<) or equal to (=).

"alarmed" State

This state means a discrete (on/off) sensor is in the "abnormal" state.

Usually for a contact closure sensor, the meaning of this state varies based on the sensor's normal state setting.

- If the normal state is set to Normally Closed, the *alarmed* state means the contact closure switch is open.
- If the normal state is set to Normally Open, the *alarmed* state means the contact closure switch is closed.

For a Raritan's floor water sensor, the normal state must be set to Normally Closed, which means no water is detected. The *alarmed* state indicates that the presence of water is detected.

Note: See **Configuring a Contact Closure Sensor** *(on page 41) for information on setting the normal state or dip switch.*

Tip: A contact closure sensor's LED is lit after entering the alarmed *state. If the sensor module has two channels for connecting two switches, two LEDs are available. Check which contact closure switch is in the "abnormal" status according to the channel number of the LED.*

"below lower critical" State

This state means a numeric sensor's reading is below the lower critical threshold as indicated below:

Reading < Lower Critical Threshold

"below lower warning" State

This state means a numeric sensor's reading is below the lower warning threshold as indicated below:

Lower Critical Threshold <= Reading < Lower Warning Threshold

---

Note: The symbol <= means smaller than (<) or equal to (=).

"above upper warning" State

This state means a numeric sensor's reading is above the upper warning threshold as indicated below:

Upper Warning Threshold <= Reading < Upper Critical Threshold

---

Note: The symbol <= means smaller than (<) or equal to (=).

"above upper critical" State

This state means a numeric sensor's reading is above the upper critical threshold as indicated below:

Upper Critical Threshold <= Reading

Note: The symbol <= means smaller than (<) or equal to (=).

Unmanaging Environmental Sensors

When it is unnecessary to monitor a particular environmental factor, you can unmanage or release the corresponding environmental sensor so that the PX device stops retrieving the sensor's reading and/or state.

To release a managed sensor:

1. If the PDU folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 83).

   Note: The PDU folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the PDU** *(on page 98).*

2. Click External Sensors in the Dominion PX Explorer pane, and the External Sensors page opens in the right pane.
3. Select the checkbox of the sensor you want to unmanage on the External Sensors page. To release multiple sensors, select the checkboxes of all desired sensors.
   - To select all environmental sensors listed on the External Sensors page, have the checkbox in the header row selected.
4. Click Release.

After a sensor is removed from management, the ID number assigned to that sensor is released and can be automatically assigned to any newly-detected sensor.

Asset Management

Configure the asset management settings only when an asset sensor is physically connected to the PX device.

Note: To set up an asset management system, see **Connecting the Asset Management Sensor (Optional)** *(on page 47).*

Configuring the Asset Sensor

The PX cannot detect how many rack units (tag ports) a connected asset management sensor supports, so you must provide this information manually.

When you add an asset management sensor, you name it.

To configure an asset sensor (asset strip):

1. If the Feature Port folder is not expanded, expand it to show the device under the Feature Port folder.
2. Click the asset sensor in the left pane. The asset sensor's page opens in the right pane.

   Note: The asset sensor is named "Asset Strip 1" by default. The name changes after being customized.

   Tip: The same asset sensor's page can be also opened by clicking Feature Port in the left pane, and then double-clicking the asset sensor in the right pane.
3. Click Setup. The setup dialog for the asset sensor appears.

   Tip: You can also trigger the same dialog by clicking Asset Management in the left pane, and then clicking Asset Strip Setup or double-clicking the asset sensor in the right pane.
4. To rename the asset sensor, type a new name in the Name field.
5. In the "Number of Rack Units" field, type the total number of rack units supported by the AMS. Default is 48.
6. Here, rack units are the number of asset management tag ports on the asset management strip. For example, if the AMS has 48 asset management tag ports, it supports up to 48 rack units on a cabinet.
7. Determine how to number all rack units on the asset sensor by selecting an option in the Numbering Mode.
   - Top-Down: The rack units are numbered in the ascending order from the highest to the lowest rack unit.
   - Bottom-Up: The rack units are numbered in the descending order from the highest to the lowest rack unit.
8. In the Numbering Offset field, select the starting number. For example, if you select 3, the first rack unit is numbered 3, the second is numbered 4, the third is numbered 5, and so on until the final number.
9. Indicate how the asset sensor is mounted on the rack in the Orientation field. The rack unit that is most close to the RJ-45 connector of the asset sensor will be marked with the index number 1 in the web interface.

For the latest version of asset sensors with a built-in tilt sensor, it is NOT necessary to configure the orientation setting manually. The PX device can detect the orientation of the asset sensors and automatically configure it.

- Top Connector: This option indicates that the asset sensor is mounted with the RJ-45 connector located on the top.

10. Bottom Connector: This option indicates that the asset sensor is mounted with the RJ-45 connector located at the bottom. Click OK to save the changes.

Setting Asset Sensor LED Colors

Each LED on the asset sensor indicates the presence and absence of a connected asset tag by changing its color. You can configure or change the color settings for all LEDs on the connected asset sensor(s) by following the procedure below.

This feature is accessible only by users with Administrative Privileges.

To configure all LED colors:

1. Connect the asset sensor to the PX if it is not already.
2. Click on the Feature Ports folder in the navigation tree to expand it.
3. Click the desired asset sensor. The page specific to that asset sensor opens in the right pane, showing the asset sensor settings and information of all rack units (tag ports).

   Note: You can also access this dialog by double-clicking the asset sensor shown on the Dashboard page.

4. Click Setup on the asset sensor page. The setup dialog for that asset sensor appears.
5. To change the LED color denoting the absence of a connected tag, either click a color in the color palette or type the hexadecimal RGB value of the color in the "Color without connected Tag" field.
6. Click OK to save the changes.

Tip: To make a specific LED's color settings different from other LEDs, see **Configuring a Specific Rack Unit** *(on page 235).*

Configuring a Specific Rack Unit

In the PX web interface, a rack unit refers to a tag port on the asset sensor. You can name a specific rack unit, or change its LED color settings so that this LED behaves differently from others on the same asset sensor.

To configure a specific rack unit:

1. If the Feature Port folder is not expanded, expand it to show the device under the Feature Port folder.
2. Click the asset sensor in the left pane. The asset sensor's page opens in the right pane.

   Note: The asset sensor is named "Asset Strip 1" by default. The name changes after being customized.

   Tip: The same asset sensor's page can be also opened by clicking Feature Port in the left pane, and then double-clicking the asset sensor in the right pane.
3. Select the rack unit whose LED settings you want to change.
4. Click Configure Rack Unit or double-click the selected rack unit. The setup dialog for the selected rack unit appears.
5. In the Name field, type a name for identifying this rack unit.
6. Select either Auto or Manual Override as this rack unit's LED mode.
   - Auto (based on Tag): This is the default setting. With this option selected, the LED follows the global LED color settings.
   - Manual Override: This option differentiates this LED's behavior. After selecting this option, you must select an LED mode and/or an LED color for the selected rack unit.
     - LED Mode: Select On to have the LED stay lit, Off to have it stay off, "Slow blinking" to have it blink slowly, or "Fast blinking" to have it blink quickly.
     - LED Color: If you select On, "Slow blinking" or "Fast blinking" in the LED Mode field, select an LED color by either clicking a color in the color palette or typing the hexadecimal RGB value of a color in the accompanying text box.
7. Click OK to save the changes.

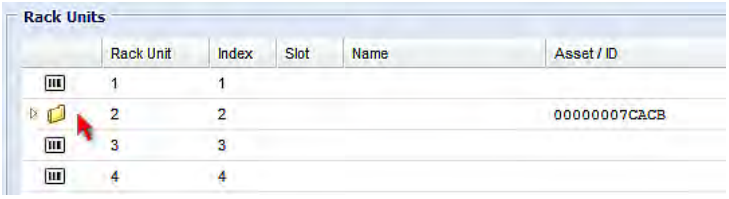
Expanding a Blade Extension Strip

A blade extension strip, like an asset sensor, has multiple tag ports. After connecting it to a specific asset sensor, it is displayed as a folder on that asset sensor's page.

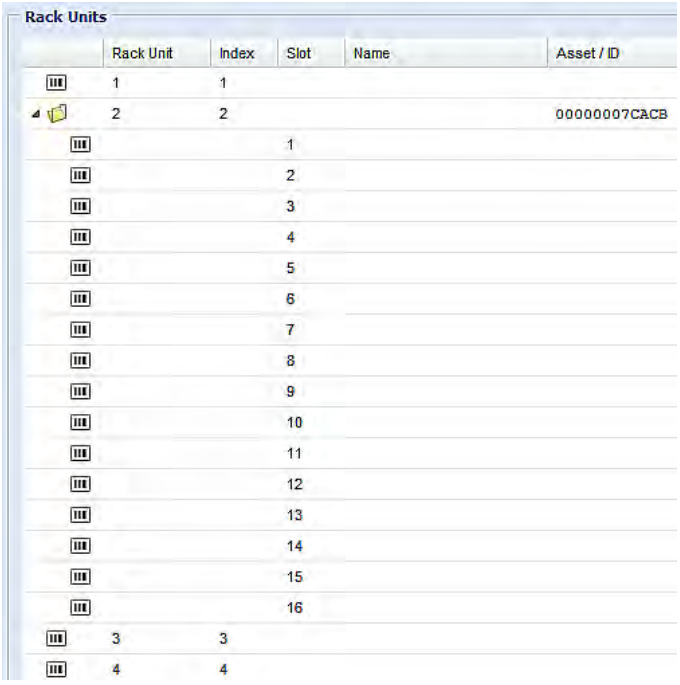
Note: If you need to temporarily disconnect the tag connector of the blade extension strip, wait at least 1 second before connecting it back, or the PX may not detect it.

To expand a blade extension strip folder:

1. Click the desired asset sensor in the left pane. The selected asset sensor's page opens in the right pane.
2. Locate the rack unit (tag port) where the blade extension strip is connected.



3. Double-click that rack unit or click the white arrow ▷ prior to the folder icon. The arrow then turns into a black, gradient arrow ◢, and all tag ports appear below the folder.



To collapse a blade extension strip:

- Double-click the blade extension strip folder, or click the black, gradient arrow ◢ prior to the folder icon. All tag ports under the folder are hidden.

Displaying the Asset Sensor Information

The hardware and software information of the connected asset sensor is available through the web interface.

To display the asset sensor information:

1. Connect the asset sensor to the PX if it is not already.
2. Click on the Feature Ports folder in the navigation tree to expand it.
3. Click the desired asset sensor. The page specific to that asset sensor opens in the right pane, showing the asset sensor settings and information of all rack units (tag ports).

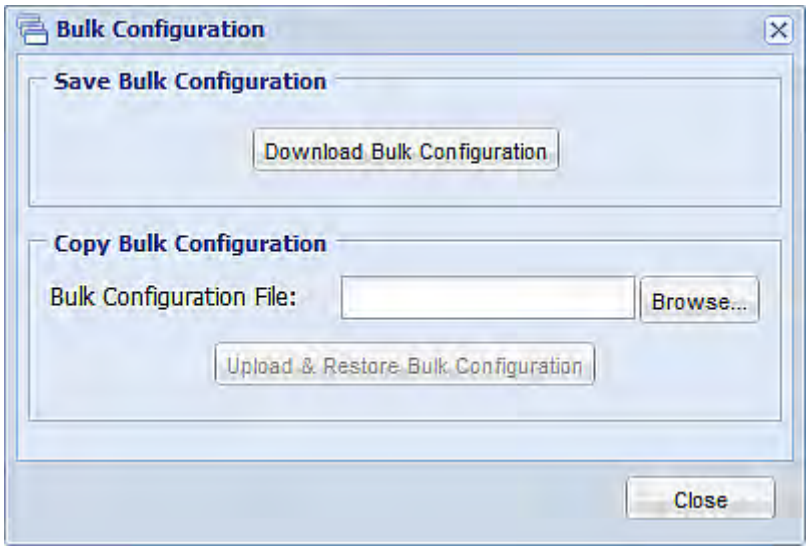
   Note: You can also access this dialog by double-clicking the asset sensor shown on the Dashboard page.

4. Click Extended Device Info, where the asset sensor data is displayed.
5. Click Close to quit the dialog.

Bulk Configuration

The Bulk Configuration feature lets you save the settings of a configured PX device to your PC. You can use this configuration file to copy that configuration to other PX devices of the same model and firmware version.

You must have the administrator privileges to save and copy the PX configurations.



Note: No device-specific data is saved to the Bulk Configuration file, such as environmental sensor or certain network settings. To back up or restore a specific PX device's settings, use the Backup/Restore feature instead. See **Backup and Restore of PX Device Settings** *(on page 240).*

Saving a PX Configuration

A source device is an already configured PX device that is used to create a configuration file containing the settings that can be shared between PX devices. These settings include user and role configurations, thresholds, event rules, security settings, and so on.

This file does NOT contain device-specific information, including:

- Device name
- System name, system contact and system location
- Network settings (IP address, gateway, netmask and so on)
- Device logs
- Outlet names
- Outlet status
- Environmental sensor names
- Environmental sensor states and values
- SSL certificate

Because the date and time settings are saved in the configuration file, users should exercise caution when distributing the configuration file to the PX devices in a different time zone than the source device.

To save a configuration file:

1. Choose Maintenance > Bulk Configuration. The Bulk Configuration dialog appears.
2. Click Download Bulk Configuration.
3. When the web browser prompts you to open or save the configuration file, click Save. Choose a suitable location and save the configuration file to your PC.

The file is saved in the XML format, and its content is encrypted using the AES-128 encryption algorithm.

Copying a PX Configuration

A target device is an PX device that loads another PX device's configuration file.

Copying an PX configuration to a target device adjusts that PX device's settings to match those of the source PX device. In order to successfully copy an PX configuration:

- The user must be the Admin user. Or the Admin role is assigned to the user.
- The target PX device must be of the same model type as the source PX device.
- The target PX device must be running the same firmware version as the source PX device.

To copy a PX configuration:

1. Log in to the target device's web interface.
2. If the target device's firmware version does not match that of the source device, update the target's firmware. See ***Firmware Upgrade*** (on page 258).
3. Choose Maintenance > Bulk Configuration. The Bulk Configuration dialog appears.
4. In the Copy Bulk Configuration section, click Browse and select the configuration file stored on your PC.
5. Click Upload & Restore Bulk Configuration to copy the file.

   A message appears, prompting you to confirm the operation and enter the admin password.
6. Enter the admin password, then click Yes to confirm the operation.
7. Wait until the PX device resets and the Login page re-appears, indicating that the configuration copy is complete.

Backup and Restore of PX Device Settings

Different from the Bulk Configuration file, the backup file contains device-specific data like network settings. To back up or restore the PX device settings, you should perform the Backup/Restore feature.

All PX information is captured in the XML backup file except for the device logs and SSL certificate.

To download a backup PX XML file:

1. Choose Maintenance > Backup/Restore. The Backup/Restore of Device Settings dialog opens.

2. In the Save Device Settings section, click Download Device Settings. Save the file to your computer.

   The file is saved in the XML format, and its content is encrypted using the AES-128 encryption algorithm.

To restore the PX using a backup XML file:

1. Choose Maintenance > Backup/Restore. The Backup/Restore of Device Settings dialog opens.
2. In the Copy Device Settings section, click Browse to locate the file.
3. Click Upload & Restore Device Settings to upload the file.

   A message appears, prompting you to confirm the operation and enter the admin password.
4. Enter the admin password, then click Yes to confirm the operation.
5. Wait until the PX device resets and the Login page re-appears, indicating that the restore is complete.

Note: To do the bulk configuration among multiple PX devices, perform the Bulk Configuration feature instead. See **Bulk Configuration** *(on page 238).*

Webcam Management

With a Logitech® webcam connected to the PX device, you can visually monitor the environment around the PX via snapshots or videos captured by the webcam.

For more information on the Logitech webcam, see the user documentation accompanying it. For information on connecting a webcam to the PX, see ***Connecting a Logitech Webcam (Optional)*** (on page 58).

Snapshots or videos captured by the webcam are displayed in the right pane of PX web interface once a webcam is selected in the navigation tree. Snapshots and videos can also be displayed in Live Preview mode in the Primary Standalone Live Preview window by clicking on the Live Preview icon .

You must have Change Webcam Configuration permission applied to your role in order to configure webcams, and the View Webcam Images and Configuration permission to view images in PX.

You can manually store snapshots taken from the webcam. See ***Saving Snapshots*** (on page 246).

Links to snapshots or videos being captured by a webcam can be sent via email or instant message. See ***Sending Snapshots or Videos in an Email or Instant Message*** (on page 244).

Events that trigger emails containing snapshots from a webcam can be created. See ***Creating Actions*** (on page 181).

Configuring Webcams

Before you can configure a webcam, it must be connected to the PX. See ***Connecting a Logitech Webcam (Optional)*** (on page 58).

To configure a webcam:

1. In the navigation tree, click on the Webcam Management folder. The Webcam Management page opens.
2. Click on the webcam you want to configure and then click Setup at the bottom right of page. The Webcam Setup dialog opens.
3. Enter a name for the webcam. Up to 64 characters are supported.
4. Select a resolution for the webcam.
5. Select the webcam mode. This can be changed as needed once the webcam is configured.
   a. Video - the webcam is in video mode. Set the Framerate (frames per second) rate.

b. Snapshot - the webcam displays images from the webcam. Set the Time Between Image(s) rate as measured in seconds.

6. Click OK. The image or video from the webcam is now available in the PX once you click on the webcam in the navigation tree.

To edit a webcam configuration:

1. In the navigation tree, click on the Webcam Management folder. The Webcam Management page opens.
2. Double-click on the webcam you want to edit. The webcam image or video opens in a new tab.
3. Click Setup.
4. Edit the information as needed. Changes to the resolution do not apply to existing, stored images - it applies only to images and videos taken after the resolution is changed.
5. Click OK.

Adjusting Snapshot or Video Properties

If any snapshot or video properties, such as the brightness, contrast, saturation, and gain settings, do not satisfy your needs, adjust them in the Webcam Setup dialog.

To adjust the image or video properties:

1. Click on the webcam shown on the Webcam Management page or in the navigation tree. See ***Configuring Webcams*** (on page 242).
2. Click Setup.
3. Click the Controls tab.
4. Adjust the desired property by adjusting the corresponding slide bar.

Viewing the Webcam Snapshots or Videos

With a Logitech® webcam connected to the PX device, you can visually monitor the environment around the PX via snapshots or videos captured by the webcam.

The PX allows you to switch between snapshots or live videos being captured by the webcam.

To switch between the snapshot and video mode:

1. Click the Webcam icon in the navigation tree.

Note: A Webcam icon appears only when a supported Logitech® webcam is connected to the PX. See **Connecting a Logitech Webcam (Optional)** *(on page 58).*

2. By default the PX enters the snapshot mode. Wait around one minute for the snapshot to appear. In the snapshot mode, a snapshot mode icon appears on the top-left corner of the image. The webcam's location information, if available, is displayed in the Location pane below the image.
   - To change the image resolution, click Setup and select a different resolution from the Resolution drop-down list. The displayed image is updated with the latest snapshot when the resolution changes.
   - To save the snapshot being displayed, click the Store Snapshot to Webcam Storage icon. See ***Saving Snapshots*** (on page 246).
3. To switch to the video mode, do the following:
   a. Click Setup.
   b. In the Webcam Mode field, select Video.

   In the video mode, a video mode icon appears on the top-left corner of the image.
   - To change the video resolution, click Setup and select a different resolution from the Resolution drop-down list.
4. To return to the snapshot mode, do the following:
   a. Click Setup.
   b. In the Webcam Mode field, select Snapshot.

Sending Snapshots or Videos in an Email or Instant Message

You are able to email or instant message up to two (2) recipients a link to webcams attached to the PX. Users can then click on the links and view snapshots or videos.

Note: For remote Live Preview sessions, such as those accessed via link in an email or instant message, a total of up to three (3) simultaneous Live Preview sessions are supported at a time. One (1) from the originator in the PX interface, and up to two (2) remote sessions.

Note: For the purposes of this topic, the message sender is User A and the recipient is User B.

The recipient is able to access the snapshot or video image via the link so long as either:

- The snapshot or video remains open in Live Preview mode in the User A's PX interface, and User A does not log out of the interface and the session does not time out.

  Or

- The snapshot or video remains open in a secondary Live Preview window in the User A's PX interface. So long as the secondary Live Preview window is open in User A's interface, even after User A logs out of the PX interface or the session times out, the link is available.

Best Practice

As a best practice, in the PX interface, User A should open the snapshot or video in a secondary Live Preview window and leave the Live Preview window open at least until User B opens the snapshot or video via the link.

Once User B opens the snapshot or video via the link, the secondary Live Preview mode window can be closed in the User A's PX interface.

User B can either manually let User A know they have opened the link, or User A can check to see if User B is currently connected to the application by choosing Maintenance > Connected Users.

To send a snapshot or video link via email or instant message:

1. In the navigation tree, click on the webcam that is capturing the snapshot or video you want to provide a link to in the email. The snapshot or video is displayed in Live Preview mode in the right pane.
2. Click on the Live Preview icon located above the snapshot or video. The snapshot or video opens in a secondary Live Preview window.
3. Copy the URL from the Live Preview window, paste it into the email or instant message application. Leave the Live Preview window open at least until the recipient opens the snapshot or video via the link.

Snapshot Storage

Once a snapshot is taken using the Store Snapshot to Webcam Storage feature, it is stored locally on the PX. Up to ten (10) images can be stored on the PX at once. Unless snapshots are deleted manually, the oldest snapshot is automatically deleted from the device when the number of snapshots exceeds ten.

Note: Rebooting the PX deletes the snapshots taken via webcam.

To save more than 10 snapshots, save the images on a Common Internet File System/Samba.

Note: NFS and FTP are not supported for this release and are disabled on the dialog.

See ***Configuring Webcam Storage*** (on page 247) for more information on configuration an image storage location.

Snapshot files are saved as JPG files. The snapshot file is named based on the number of the snapshot starting from 1. So the first snapshot that is taken is named 1.jpg, the second is 2.jpg and so on.

Saving Snapshots

If it is intended to keep the currently-displayed webcam snapshot, you can manually save it onto the PX. A snapshot is saved as a JPEG file and stored on the Snapshots page.

Warning: The stored snapshots are lost when you reset the PX so make sure it is fine to clear up the stored snapshots before performing the reset.

To save the snapshot being displayed:

1. In the navigation tree, click on the webcam you want to take a snapshot with. The webcam image is displayed in the right pane.

   The webcam must be in snapshot mode in order to take snapshots. If the webcam is in video mode, click Setup in the right pane above the video image to open the Webcam Setup dialog, then select the Snapshot radio button.

2. Once the snapshot image being taken by the selected webcam is displayed in the right pane, click the Store Snapshot to Webcam Storage icon above the image to take a snapshot. Up to ten (10) snapshots can be stored at once on the device.

3. Click on the Snapshots icon in the navigation tree to verify that the snapshot is successfully saved and listed on the Snapshots page.

Managing the Snapshots Saved to PX

A maximum of 10 saved snapshots are listed and displayed on the Snapshots page of the PX.

The Snapshots page is split into three sections: Storage, Snapshot and Details.

- Storage: shows a list of all saved snapshots. On the top of the Storage section, it indicates the total number of saved snapshots (Used) and the maximum number of snapshots allowed (Size) in storage.
- Snapshot: displays the image of the snapshot being selected.
- Details: shows the information which had been entered when the snapshot was saved.

To view the saved snapshots:

1. In the navigation tree, click Snapshot under the Webcam Management folder. The snapshots are displayed in the right pane in the Storage section of the page.
2. View an individual snapshot by clicking on a snapshot file in the Storage section of the page.

The size of each snapshot file, the date and time each snapshot was taken, and the webcam that took each snapshot, is displayed when viewing snapshots.

Details, such as the webcam location and/or labels, if any, are displayed in the Details section below the snapshot in the right pane. This information is defined when the webcam is initially configured. See ***Configuring Webcams*** (on page 242).

To delete any snapshot from the storage:

- Delete snapshots by selecting the checkbox next to the snapshot you want to delete, then clicking the Delete icon at the top of the section. To select and delete all snapshots at once, click the checkbox in the checkbox column header, then click the Delete icon.

To change the sorting or displayed columns of the list:

- You can resort the snapshot list or hide any displayed column in the Storage section. For details, see ***Changing the View of a List*** (on page 90).

Configuring Webcam Storage

By default, when a snapshot is taken using the Store Snapshot to Webcam Storage feature, it is stored locally on the PX. Up to ten (10) images can be stored on the PX at once.

To save more than 10 snapshots, save the images on a Common Internet File System/Samba.

Note: NFS and FTP are not supported for this release and are disabled on the dialog.

To configure another storage location for images:

1. In the navigation tree, click Snapshot under the Webcam Management folder. The Snapshots page opens.
2. Click on the Setup Storage icon . The Storage Setup dialog opens.
3. By default, Local, meaning the PX, is the designated default storage.
4. Select CIFS/Samba as the storage location.
5. Enter the server on which to store the images.
6. If needed, enter the share drive/folder to store the images in.
7. Enter the username and password needed to access the server the images are stored on.
8. Enter or use the slide bar to set the number of images that can be saved to the storage location.
9. Click OK.

Network Diagnostics

The PX provides the following tools in the web interface for diagnosing potential networking issues.

- Ping
- Trace Route
- List TCP Connections

Tip: These network diagnostic tools are also available through CLI. See **Network Troubleshooting** *(on page 442).*

Pinging a Host

The Ping tool is useful for checking whether a host is accessible through the network or Internet.

To ping a host:

1. Choose Maintenance > Network Diagnostics > Ping. The Ping Network Host dialog appears.
2. In the Host Name field, type the name or IP address of the host that you want to check.
3. In the Number of Requests field, type a number up to 10 or adjust the value by clicking either arrow. This number determines how many packets are sent for pinging the host.
4. Click Run Ping to start pinging the host. A dialog appears, displaying the Ping results.
5. Click Close to quit the dialog.

Tracing the Network Route

Trace Route lets you find out the route over the network between two hosts or systems.

To trace the route for a host:

1. Choose Maintenance > Network Diagnostics > Trace Route. The Trace Route to Host dialog appears.
2. Type the IP address or name of the host whose route you want to check in the Host Name field.
3. Click Run. A dialog appears, displaying the Trace Route results.
4. Click Close to quit the dialog.

Listing TCP Connections

You can use the "List TCP Connections" to display a list of TCP connections.

To trace the route for a host:

1. Choose Maintenance > Network Diagnostics > List TCP Connections. The TCP connections dialog appears.
2. Click Close to quit the dialog.

Viewing the Communication Log

The PX allows you to inspect all communications occurred between the PX device and its graphical user interface (GUI). The information is usually useful for a technical support engineer only and you may not need to view it.

This feature is accessible only by users with Administrative Privileges.

To view the communication log:

1. Choose Maintenance > View Communication Log. The Communication Log dialog appears.
2. The dialog shows the final page by default. You can:
   - Switch between different pages by doing one of the following:

     - Click or to go to the first or final page.

     - Click or to go to the prior or next page.

     - Type a number in the Page text box and press Enter to go to a specific page.
   - Select a log entry from the list and click Show Details, or simply double-click the log entry to view detailed information.

   Note: Sometimes when the dialog is too narrow, the icon takes the place of the Show Details button. In that case, click and select Show Details to view details.

   Click to view the latest events.
3. To save the communication log on your computer, click .
4. To clear all records in the communication log, click Clear Communication Log. Click Yes on the confirmation message.

Downloading Diagnostic Information

Important: This function is for use by Raritan Field Engineers or when you are directed by Raritan Technical Support.

You can download the diagnostic file from the PX device to a client machine. The file is compressed into a .tgz file and should be sent to Raritan Technical Support for interpretation.

This feature is accessible only by users with Administrative Privileges.

To retrieve a diagnostic file:

1. Choose Maintenance > Download Diagnostic Information. The File Download dialog appears.

File Download
Do you want to open or save this file?
Name: diag-data.tgz
Type: WinRAR archive
From: 192.168.84.57
Open
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

2. Click Save. The Save As dialog appears.
3. Navigate to the desired directory and click Save.
4. E-mail this file as instructed by Raritan Technical Support.

Managing the Schroff LHX Heat Exchanger

The PX supports monitoring and administering the Schroff® LHX-20 or LHX-40 heat exchanger if this device is connected to the PX.

From the PX, you can remotely do the following:

- Name a connected LHX heat exchanger
- Configure the air outlet temperature setpoint
- Configure air outlet temperature thresholds
- Configure air inlet temperature thresholds
- Configure water inlet temperature thresholds
- Configure fan speed thresholds
- Monitor the air inlet temperature
- Monitor the air outlet temperature
- Monitor the fan speed
- Configure the default fan speed to operate from 50% to 90% (the factory default is 80%)
- Request maximum cooling using the fan speed and opening the cold water valve
- Acknowledge alerts remotely (for example, return to normal operation after maximum cooling is requested)

To monitor one LHX heat exchanger using the PX:

1. Physically connect an LHX-20 or LHX-40 heat exchanger to the PX device if it is not already connected. See ***Connecting a Schroff LHX Heat Exchanger (Optional)*** (on page 59).
2. Enable the support of LHX heat exchanger on the PX. See ***Enabling and Disabling Schroff LHX Heat Exchanger Support*** (on page 252).
3. Configure the connected heat exchanger. See ***Configuring the LHX Device*** (on page 252).
4. Now you can remotely monitor or control the connected LHX heat exchanger via the PX.
   - To monitor the heat exchanger, see ***Monitoring the LHX Device*** (on page 254).
   - To control the heat exchanger, see ***Turning the LHX On or Off*** (on page 257).

Enabling and Disabling Schroff LHX Heat Exchanger Support

By default, Schroff LHX Heat Exchanger support is disabled. As such, support needs to be enabled before the device appears in the navigation tree or on the dashboard. Additionally, Schroff LHX Heat Exchanger support must be enabled in order for the LHX-MIB to be accessible through SNMP.

To enable the Schroff LHX Heat Exchanger:

1. Select Device Settings > Features, and then select the Schroff Heat Exchanger checkbox on the menu.
2. Click Yes to confirm.
3. Reboot the PX.

Configuring the LHX Device

After enabling the LHX support on the PX, the PX should automatically detect the connected LHX device and display it under the Feature Port folder unless the Feature Port is set to a mode different than the Auto mode. If so, change the Feature Port mode so that the LHX device is correctly displayed in the web interface. See ***Configuring the Feature Port*** (on page 113).

Besides, the PX allows you to set temperature or fan speed thresholds for alerts or to customize the name of the LHX device for easy identification.

Correctly Displaying the LHX Device

There are two ways to have the PX show the correct LHX model in the web interface.

- Auto detection: Set the mode of the Feature Port to Auto to let the PX automatically detects the device type.
- Manual assignment: Set the mode of the Feature Port to either LHX-20 or LHX-40, depending on which LHX model is physically connected to the PX.

For details on how to change the Feature Port mode, see ***Configuring the Feature Port*** (on page 113).

After the correct LHX device type is detected or assigned, the LHX icon appears below the Feature Port folder.

Note that the device icon changes its image when the device changes its states. See ***Device States and Icon Variations*** (on page 255) for details.

Setting Up an LHX

Once an LHX heat exchanger is connected, you can setup the device by giving it a name, and configuring its setpoint air outlet and default fan speed.

To set up the LHX:

1. If the Feature Port folder is not expanded, expand it to show the device under the Feature Port folder.
2. Click the LHX heat exchanger in the Dominion PX Explorer pane. The page specific to that device opens in the right pane.
3. Click Setup in the Settings section of the page. The Setup dialog opens.
4. Type a name for the heat exchanger in the Name field. The customized LHX heat exchanger's name is followed by the device type in parentheses.
5. Enter the air outlet's temperature set point in the Setpoint Air Outlet (°C) field.
6. Enter the default fan speed in the Default Fan Speed (%) field.
7. Click OK.

Configuring Temperature and Fan Thresholds

An LHX heat exchanger is implemented with various sensors for detecting the air temperature, water temperature, and fan speed. You can set thresholds for these sensors so that the PX alerts you when any sensor readings are getting close to a critical condition. These settings are stored on the PX port where the heat exchanger is connected, and are lost if that heat exchanger is moved to a different port.

To configure the thresholds for a sensor:

1. Connect the LHX heat exchanger to PX if it is not already connected.
2. If the Feature Port folder is not expanded, expand it to show the device under the Feature Port folder.
3. Click the LHX heat exchanger in the Dominion PX Explorer pane. The page specific to that device opens in the right pane.
4. Select the desired sensor in the Sensors table and click Setup Thresholds, or simply double-click that sensor. The setup dialog for the selected sensor appears.
5. Adjust the threshold and deassertion hysteresis settings. The Upper Critical and Lower Critical values are points at which the PX considers the operating environment critical and outside the range of the acceptable threshold.

- To enable any threshold, select the corresponding checkbox. To disable a threshold, deselect the checkbox.
- After any threshold is enabled, type an appropriate numeric value in the accompanying text box.
- To enable the deassertion hysteresis for all thresholds, type a numeric value other than zero in the Deassertion Hysteresis field. See ***What is Deassertion Hysteresis?*** (on page 178).

6. Click OK to save the changes.

Monitoring the LHX Device

The PX web interface lets you monitor the status of the connected LHX heat exchanger as well as the status of the LHX built-in sensor.

Viewing the Summary

Both the Dashboard and Feature Port pages display the summary of the connected LHX heat exchangers, including the heat exchanger's name and status, if the LHX device is detected or manually assigned to the Feature Port.

If the LHX heat exchanger is highlighted in red in the summary, it indicates that there is LHX sensor failure on that heat exchanger. View the State column to identify failed sensors.

To view the LHX summary on the Dashboard page:

1. Click the Dashboard icon in the Dominion PX Explorer pane. The Dashboard page opens in the right pane.
2. Locate the LHX Heat Exchanger section.

To view the LHX summary on the Feature Port page:

1. If the PDU folder is not expanded, expand it to show all components and component groups. See ***Expanding the Tree*** (on page 83).

   Note: The PDU folder is named "my PX" by default. The name changes after customizing the device name. See **Naming the PDU** *(on page 98).*

2. Click the Feature Port folder. The Feature Port page opens in the right pane, showing the connected LHX device information.

Viewing Details

An LHX heat exchanger page shows detailed information, including:

- Device information and settings
- The air outlet temperature
- The default fan speed
- Readings and states of all LHX built-in sensors
- Alerts and errors, such as failed LHX sensors or emergency cooling activation
- Accumulative operating hours

To view details of a specific LHX heat exchanger:

1. If the Feature Port folder is not expanded, expand it to show the device under the Feature Port folder.
2. Click the LHX icon in the left pane. The LHX page opens in the right pane.

Tip: The same LHX page can be also opened by clicking Feature Port in the left pane, and then double-clicking the LHX in the right pane.

If any LHX sensor reading reaches or crosses the critical or warning threshold, that sensor reading row is highlighted in red or yellow. See ***The Yellow- or Red-Highlighted Reading*** (on page 89).

Device States and Icon Variations

The PX web interface changes icons to represent different statuses of the connected LHX heat exchanger.

Icons	Device status
	The heat exchanger is turned ON and operating normally.
	The heat exchanger is turned OFF.
	The heat exchanger is turned ON but enters the critical state because of any LHX sensor failure.
	At least one of the LHX sensor readings has crossed the upper or lower warning threshold.
	NO LHX device is detected on the FEATURE port.

To identify the cause of the critical state, view one of the following.

- The LHX Heat Exchanger section of the Dashboard page. See ***Viewing the Summary*** (on page 254).
- The Feature Port page. See ***Viewing the Summary*** (on page 254).
- The Alert States section of the LHX heat exchanger page. See ***Alert States and LHX Event Log*** (on page 256).

Alert States and LHX Event Log

When an LHX heat exchanger is physically connected to the PX device, a section labeled Alert States appears on its device page. The Alert States section shows information identifying the LHX sensors that currently fail.

Tip: The Dashboard and Feature Port pages also point out failed sensors. See **Viewing the Summary** *(on page 254).*

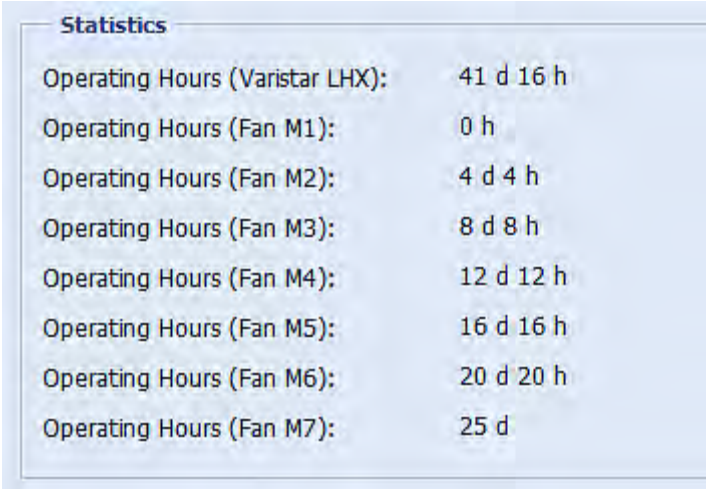
If maximum cooling of an LHX device has been requested, clicking the Acknowledge Alert Status button acknowledges the "Maximum cooling requested" alert, the message disappears from the Alerts section, the LHX returns to normal operation. See ***Requesting Maximum Cooling for an LHX*** (on page 257) for information on using the maximum cooling request feature.

A button labeled Show Event Log is located in the Alert States section. To view LHX events associated with the PX, click this button.

Operating Hours

Operating hours are the accumulative time since the LHX heat exchanger is first connected to the PX device and turned ON.

The PX web interface displays the operating hours both for the heat exchanger and its fans. Operating hour information is located in the Statistics section of each heat exchanger page.


Statistics
Operating Hours (Varistar LHX): 41 d 16 h
Operating Hours (Fan M1): 0 h
Operating Hours (Fan M2): 4 d 4 h
Operating Hours (Fan M3): 8 d 8 h
Operating Hours (Fan M4): 12 d 12 h
Operating Hours (Fan M5): 16 d 16 h
Operating Hours (Fan M6): 20 d 20 h
Operating Hours (Fan M7): 25 d

Below are the time units used for operating hours:

- h: hour(s)
- d: day(s)

For example, "3d 5h" means the total operating time is 3 days and 5 hours.

Turning the LHX On or Off

The PX allows you to remotely turn on or off a connected heat exchanger.

To control the LHX heat exchanger:

1. If the Feature Port folder is not expanded, expand it to show the device under the Feature Port folder.
2. Click the LHX heat exchanger in the Dominion PX Explorer pane. The page specific to that device opens in the right pane.
3. Locate the Information section.
   - To turn off the LHX heat exchanger, click Switch Off.
   - To turn on the LHX heat exchanger, click Switch On.
4. If you clicked Switch Off in the previous step, a dialog appears, prompting you to confirm the operation. Click Yes to turn it off or No to abort the operation.

The heat exchanger's icon shown in the web interface changes after being turned on or off. See ***Device States and Icon Variations*** (on page 255).

Requesting Maximum Cooling for an LHX

When you click Request Maximum Cooling, the LHX enters into emergency cooling mode and runs at its maximum cooling level of 100% in order to cool the device.

When maximum cooling is requested for an LHX, the message "Maximum cooling requested" is displayed in the Alerts section of the LHX page. When you click the Acknowledge Alert Status button, the alert message disappears even if the actual cooling action on the device is still underway. For additional information on the maximum cooling function, see the LHX documentation.

To request maximum cooling for an LHX:

1. If the Feature Port folder is not expanded, expand it to show the device under the Feature Port folder.
2. Click the LHX heat exchanger in the Dominion PX Explorer pane. The page specific to that device opens in the right pane.
3. Click the desired heat exchanger under the Auxiliary folder. The page specific to that heat exchanger opens in the right pane.

4. In the Information section of the page, click Request Maximum Cooling to cool the device.

Firmware Upgrade

You may upgrade your PX device to benefit from the latest enhancements, improvements and features.

The PX firmware files are available on the Raritan website's ***Firmware and Documentation section*** (***http://www.raritan.com/support/firmware-and-documentation/***).

Updating the PX Firmware

When performing the firmware upgrade, the PX keeps each outlet's power status unchanged so no server operation is interrupted. Outlets that have been powered on prior to the firmware upgrade remain powered on and outlets that have been powered off prior to the firmware upgrade remain powered off during and after the firmware upgrade.

You must be the system administrator or log in to the user profile with the Firmware Update permission to update the PX device's firmware.

If applicable to your model, download the latest firmware file from the Raritan website, read the release notes, then start the upgrade. If you have any questions or concerns about the upgrade, contact Raritan Technical Support BEFORE upgrading.

Warning: Do NOT perform the firmware upgrade over a wireless connection.

To update the firmware:

1. Choose Maintenance > Update Firmware. The Firmware Update dialog appears.
2. In the Firmware File field, click Browse to select an appropriate firmware file.
3. Click Upload. A progress bar appears to indicate the upload status.
4. When the upload is complete, version information of both the existing firmware and uploaded firmware is shown, providing you a last chance to terminate the update.
5. To view the certificate of the uploaded firmware, click View Certificate. **Optional.**
6. To proceed with the update, click Update Firmware. The update may take several minutes.

   Warning: Do NOT power off the PX device during the update.

   During the firmware update:

- A progress bar appears in the web interface, indicating the update status.
- The display on the PX device shows three digits “FUP.”
- The outlet LEDs flash when the relay boards are being updated.

Exception: If the firmware update does not include the update of the relay board firmware, outlet LEDs do NOT flash.

- No users can successfully log in to the PX.
- The user management operation, if any, is forced to suspend.

7. When the update is complete, a message appears, indicating the update is successful.
8. The PX device resets, and the Login page re-appears. You can now log in and resume your operation.

Note 1: The other logged-in users are also logged out when the firmware update is complete.

Note 2: If you are using the PX with an SNMP manager, download the PX MIB again after the firmware update to ensure your SNMP manager has the correct MIB for the latest release you are using. See ***Using SNMP*** (on page 263) in the PX User Guide.

A Note about Firmware Upgrade Time

The PDU firmware upgrade time varies from unit to unit, depending on various external and internal factors.

External factors include, but are not limited to: network throughput, firmware file size, and speed at which the firmware is retrieved from the storage location. Internal factors include: the necessity of upgrading the firmware on the microcontroller and the number of microcontrollers that require upgrade (which depends on the number of outlets). The microcontroller is upgraded only when required. Therefore, the length of firmware upgrade time ranges from approximately 3 minutes (without any microcontroller updated) to almost 7 minutes (with all microcontrollers for 48 outlets updated). Take the above factors into account when estimating the PDU's firmware upgrade time.

The time indicated in this note is for web-interface-based upgrades. Upgrades through other management systems, such as Raritan's Power IQ, may take additional time beyond the control of the PDU itself. This note does not address the upgrades using other management systems.

Viewing Firmware Update History

The firmware upgrade history, if available, is permanently stored on the PX device.

This history indicates when a firmware upgrade event occurred, the prior and new versions associated with the firmware upgrade event, and the upgrade result.

To view the firmware update history:

1. Choose Maintenance > View Firmware Update History. The Firmware Update History dialog appears, with the following information displayed.
   - Date and time of the firmware upgrade event
   - Previous firmware version
   - Update firmware version
   - Firmware upgrade result
2. You may change the number of displayed columns or re-sort the list for better viewing the data.
3. To view the details of any firmware upgrade event, select it and click Details, or simply double-click the event. The Firmware Update Details dialog appears, showing detailed information of the selected event.
4. Click Close to quit the dialog.

Full Disaster Recovery

If the firmware upgrade fails, causing the PX device to stop working, you can recover it by using a special utility rather than returning the device to Raritan.

Contact Raritan Technical Support for the recovery utility, which works in Windows XP/Vista/7 and Linux. In addition, an appropriate PX firmware file is required in the recovery procedure.

Updating the Asset Sensor Firmware

After connecting the asset sensor to the PX device, it automatically checks its own firmware version against the version of the asset sensor firmware stored in the PX firmware. If two versions are different, the asset sensor automatically starts downloading the new firmware from the PX device to upgrade its own firmware.

During the firmware upgrade, the following events take place:

- The asset sensor is completely lit up, with the blinking LEDs changing the color from red to green.
- A firmware upgrade process is indicated in the PX web interface.
- An SNMP trap is sent to indicate the firmware upgrade event.

Accessing the Help

The Help menu provides:

- Current firmware and software packages information
- A link to the PX User Guide (that is, the online help)

Retrieving Software Packages Information

You can check the current firmware version and the information of all open source packages embedded in the PX device through the web interface.

To retrieve the embedded software packages information:

1. Choose Help > About Dominion PX. The About Dominion PX dialog appears, with a list of open source packages displayed.
2. You can click any link in the dialog to access related information or download any software package.

Browsing through the Online Help

The PX User Guide is also provided in the form of online help, and accessible over the Internet.

To use online help, Active Content must be enabled in your browser. If you are using Internet Explorer 7, you must enable Scriplets. Consult your browser help for information on enabling these features.

To use the PX online help:

1. Choose Help > User Guide. The online help opens in the default web browser.
2. To view the content of any topic, click the topic in the left pane. Then its content is displayed in the right pane.
3. To select a different topic, do any of the following:

- To view the next topic, click the Next icon in the toolbar.
- To view the previous topic, click the Previous icon.
- To view the first topic, click the Home icon.

4. To expand or collapse a topic that contains sub-topics, do the following:
   - To expand any topic, click the white arrow prior to the topic, or double-click that topic. The arrow turns into a black, gradient arrow, and sub-topics appear below the topic.
   - To collapse any expanded topic, click the black, gradient arrow prior to the topic, or double-click the expanded topic. The arrow then turns into a white arrow, and all sub-topics below that topic disappear.
5. To search for specific information, type the key word(s) or string(s) in the Search text box, and press Enter or click the Search icon to start the search.
   - If necessary, select the "Match partial words" checkbox to include information matching part of the words entered in the Search text box.

   The search results are displayed in the left pane.
6. To have the left pane show the list of topics, click the Contents tab at the bottom.
7. To show the Index page, click the Index tab.
8. To email any URL link to the currently selected topic to any person, click the "Email this page" icon in the toolbar.
9. To email your comments or suggestions regarding the user guide to Raritan, click the "Send feedback" icon.
10. To print the currently selected topic, click the "Print this page" icon.

Chapter 7 Using SNMP

This SNMP section helps you set up the PX for use with an SNMP manager. The PX can be configured to send traps or informs to an SNMP manager, as well as receive GET and SET commands in order to retrieve status and configure some basic settings.

In This Chapter

Enabling SNMP 263
Configuring Users for Encrypted SNMP v3 264
Configuring SNMP Notifications 265
SNMP Gets and Sets 269

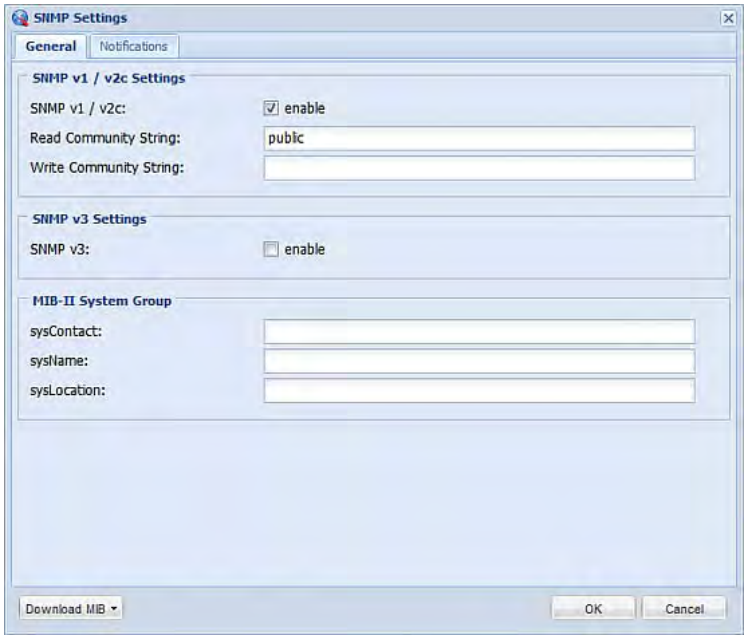
Enabling SNMP

By default, SNMP v1/v2c is enabled on the PX so the PX can communicate with an SNMP manager. If you have disabled the SNMP, it must be enabled to communicate with an SNMP manager.

Note that read-only access is enabled and the community string is public.

To enable SNMP:

1. Choose Device Settings > Network Services > SNMP. The SNMP Settings dialog appears.



2. Select the "enable" checkbox in the "SNMP v1 / v2c" field to enable communication with an SNMP manager using SNMP v1 or v2c protocol.
   - Type the SNMP read-only community string in the Read Community String field. Usually the string is "public."
   - Type the read/write community string in the Write Community String field. Usually the string is "private."
3. Select the "enable" checkbox in the "SNMP v3" field to enable communication with an SNMP manager using SNMP v3 protocol.

   Tip: You can permit or disallow a user to access the PX via the SNMP v3 protocol. See **Configuring Users for Encrypted SNMP v3** *(on page 264).*
4. Enter the MIB-II system group information, if applicable:
   a. sysContact - the contact person in charge of the system being contacted
   b. sysName - the name assigned to the system
   c. sysLocation - the location of the system
5. Select the MIB to be downloaded. The SNMP MIB for your PX is used by the SNMP manager.

   Important: You must download the SNMP MIB for your PX to use with your SNMP manager. Click Download MIB in this dialog to download the desired MIB file. For more details, see **Downloading SNMP MIB** *(on page 270).*
6. Click OK to save the changes.

Configuring Users for Encrypted SNMP v3

The SNMP v3 protocol allows for encrypted communication. To take advantage of this, users need to have an Authentication Pass Phrase and Privacy Pass Phrase, which act as shared secrets between them and the PX.

To configure users for SNMP v3 encrypted communication:

1. Choose User Management > Users. The Manage Users dialog appears.
2. Select the user by clicking it.
3. Click Edit or double-click the user. The Edit User 'XXX' dialog appears, where XXX is the user name.
4. To change the SNMPv3 access permissions, click the SNMPv3 tab and make necessary changes. For details, see Step 6 of ***Creating a User Profile*** (on page 120).

5. Click OK to save the changes. The user is now set up for encrypted SNMP v3 communication.

Configuring SNMP Notifications

The PX automatically keeps an internal log of events that occur. See ***Event Rules and Actions*** (on page 180). These events can also be used to send SNMP v2c or v3 notifications to a third-party destination.

The PX provides you with the ability to create SNMPv2c and SNMPv3 TRAP communications, or SNMPv2c and SNMPv3 INFORM communications.

SNMP TRAP communications capture and send information via SNMP, but no confirmation that the communication between the devices has succeeded is provided to the receiving device.

SNMP INFORM communications capture and send information via SNMP, and an acknowledgment that the communication was received by the receiving device is provided. If the inform communication fails, it is resent. You can define the number of times and the intervals to resend the inform communication, or leave the defaults of five (5) resends in three (3) second intervals.

Note: SNMP INFORM communications may take up slightly more network resources than SNMP TRAP communications since there are additional communications between the devices, and due to additional network traffic created should the initial communication fail and another is sent.

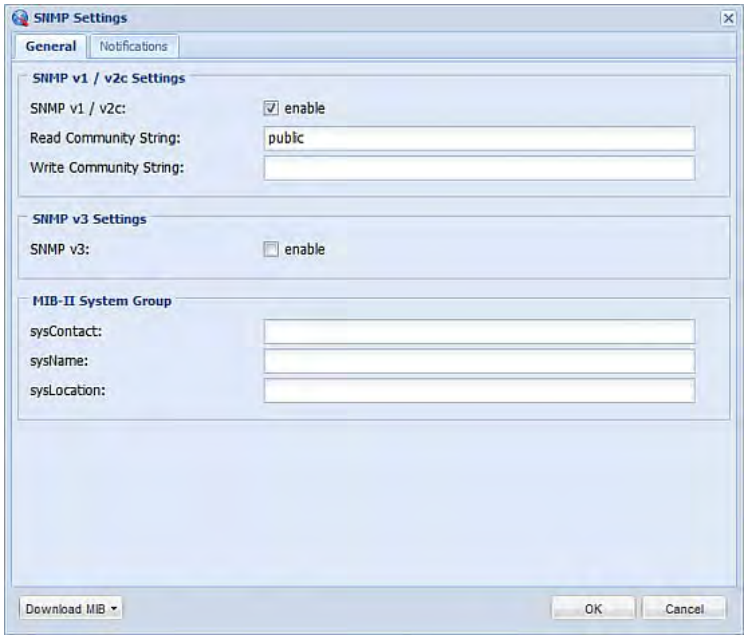
Use SNMP TRAP rules if you do not need confirmation that the communication has succeeded, and if you need to conserve network resources. Use SNMP INFORM communications to ensure more reliable communications, and if network resources can be managed with the potential additional network traffic.

Note: You should update the MIB used by your SNMP manager when updating to a new PX release. This ensures your SNMP manager has the correct MIB for the release you are using. See **Downloading SNMP MIB** *(on page 270).*

SNMPv2c Notifications

To configure the PX to send SNMP notifications:

1. Choose Device Settings > Network Services > SNMP. The SNMP Settings dialog appears.



2. Enter the MIB-II system group information, if applicable:
   a. sysContact - the contact person in charge of the system being contacted
   b. sysName - the name assigned to the system
   c. sysLocation - the location of the system
3. Select the MIB to be downloaded. The SNMP MIB for your PX is used by the SNMP manager.

   Important: You must download the SNMP MIB for your PX to use with your SNMP manager. Click Download MIB in this dialog to download the desired MIB file. For more details, see **Downloading SNMP MIB** *(on page 270).*

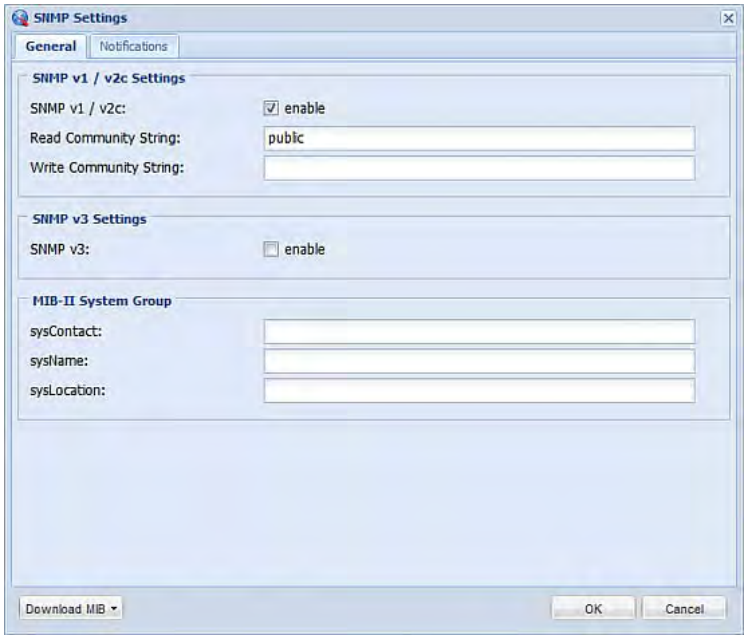
4. Click OK to save the changes.
5. On the Notifications tab, select the Enable checkbox to enable the SNMP notification feature.
6. From the Notification Type drop-down, select the type of SNMP notification.

7. For SNMP INFORM communications, leave the resend settings at their default or:
   a. In the Timeout (sec) field, enter the interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.
   b. In the Number of Retries field, enter the number of times you want to resend the inform communication if it fails. For example, inform communications are resent up to 5 times when the initial communication fails.
8. In the Host fields, enter the IP address of the device(s) you want to access. This is the address to which notifications are sent by the SNMP system agent. You can specify up to 3 SNMP destinations.
9. In the Port fields, enter the port number used to access the device(s).
10. In the Community fields, enter the SNMP community string to access the device(s). The community is the group representing the PX and all SNMP management stations.
11. Click OK.

SNMPv3 Notifications

To configure the PX to send SNMPv3 notifications:

1. Choose Device Settings > Network Services > SNMP. The SNMP Settings dialog appears.



2. Enter the MIB-II system group information, if applicable:

a. sysContact - the contact person in charge of the system being contacted

b. sysName - the name assigned to the system

c. sysLocation - the location of the system

3. Select the MIB to be downloaded. The SNMP MIB for your PX is used by the SNMP manager.

Important: You must download the SNMP MIB for your PX to use with your SNMP manager. Click Download MIB in this dialog to download the desired MIB file. For more details, see **Downloading SNMP MIB** *(on page 270).*

4. Click OK to save the changes.
5. On the Notifications tab, select the Enable checkbox to enable the SNMP notification feature.
6. From the Notification Type drop-down, select the type of SNMP notification.
7. For SNMP TRAPs, the engine ID is prepopulated.
8. For SNMP INFORM communications, leave the resend settings at their default or:

a. In the Timeout (sec) field, enter the interval of time, in seconds, after which a new inform communication is resent if the first is not received. For example, resend a new inform communication once every 3 seconds.

b. In the Number of Retries field, enter the number of times you want to resend the inform communication if it fails. For example, inform communications are resent up to 5 times when the initial communication fails.

9. For both SNMP TRAPS and INFORMS, enter the following as needed and then click OK to apply the settings:

a. Host name

b. Port number

c. User ID needed to access the host

d. Select the host security level

Security level	Description
"noAuthNoPriv"	Select this if no authorization or privacy protocols are needed. • Click OK
"authNoPriv"	Select this if authorization is required but no privacy protocols are required. • Select the authentication protocol - MD5 or SHA • Enter the authentication passphrase and then confirm the authentication passphrase • Click OK
"authPriv"	Select this if authentication and privacy protocols are required. • Select the authentication protocol - MD5 or SHA • Enter the authentication passphrase and confirm the authentication passphrase • Select the Privacy Protocol - DES or AES • Enter the privacy passphrase and then confirm the privacy passphrase • Click OK

SNMP Gets and Sets

In addition to sending traps, the PX is able to receive SNMP get and set requests from third-party SNMP managers.

- Get requests are used to retrieve information about the PX, such as the system location, and the current on a specific outlet.
- Set requests are used to configure a subset of the information, such as the SNMP system name.

Note: The SNMP system name is the PX device name. When you change the SNMP system name, the device name shown in the web interface is also changed.

The PX does NOT support configuring IPv6-related parameters using the SNMP set requests.

Valid objects for these requests are limited to those found in the SNMP MIB-II System Group and the custom PX MIB.

The PX MIB

The SNMP MIB file is required for using your PX device with an SNMP manager. An SNMP MIB file describes the SNMP functions.

Downloading SNMP MIB

The SNMP MIB file for the PX can be easily downloaded from the web interface. There are two ways to download the SNMP MIB file.

To download the file from the SNMP Settings dialog:

1. Choose Device Settings > Network Services > SNMP. The SNMP Settings dialog appears.
2. Click Download MIB. A submenu of MIB files appear.
3. Select the desired MIB file to download.
   - PDU2-MIB: The SNMP MIB file for PX's power management.
   - ASSETMANAGEMENT-MIB: The SNMP MIB file for asset management.
4. Click Save to save the file onto your computer.

To download the file from the Device Information dialog:

1. Choose Maintenance > Device Information. The Device Information dialog appears.
2. Click the PDU2-MIB or ASSETMANAGEMENT-MIB link to download the desired SNMP MIB file.
   - PDU2-MIB: The SNMP MIB file for PX's power management.
   - ASSETMANAGEMENT-MIB: The SNMP MIB file for asset management.

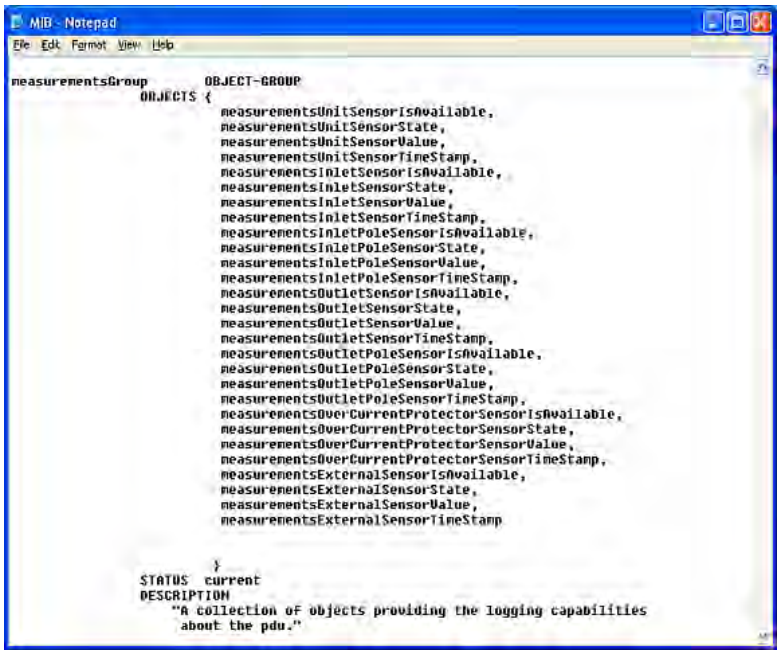
   The "USB Console INF file" link lets you download the USB-to-serial driver that may be required only when the PX is connected to a computer via an USB cable for configuration. See ***Installing the USB-to-Serial Driver (Optional)*** (on page 18) for details.
3. Click Save to save the file onto your computer.

Note: If the LHX support has been enabled, LHX-MIB is available for download in either dialog.

Layout

Opening the MIB reveals the custom objects that describe the PX system at the unit level as well as at the individual-outlet level.

As standard, these objects are first presented at the beginning of the file, listed under their parent group. The objects then appear again individually, defined and described in detail.



For example, the measurementsGroup group contains objects for sensor readings of PX as a whole. One object listed under this group, measurementsUnitSensorValue, is described later in the MIB as "The sensor value". pduRatedCurrent, part of the configGroup group, describes the PDU current rating.

SNMP Sets and Thresholds

Some objects can be configured from the SNMP manager using SNMP set commands. Objects that can be configured have a MAX-ACCESS level of "read-write" in the MIB.

These objects include threshold objects, which causes the PX to generate a warning and send an SNMP notification when certain parameters are exceeded. See ***Setting Power Thresholds*** (on page 173) for a description of how thresholds work.

Note: When configuring the thresholds via SNMP set commands, ensure the value of upper critical threshold is higher than that of upper warning threshold.

Configuring NTP Server Settings

Using SNMP can change the following NTP server-related settings:

- Enable or disable synchronizing the PDU's date and time with NTP servers.
- Enable or disable the use of DHCP-assigned NTP servers if synchronization with NTP servers is enabled.
- Manually assign the primary NTP server if the use of DHCP-assigned NTP servers is disabled.
- Manually assign the secondary NTP server (optional).

Tip: To specify the time zone, use the CLI or web interface instead. For the CLI, see **Setting the Time Zone** *(on page 342). For the web interface, see* **Setting the Date and Time** *(on page 110).*

When using the SNMP SET command to specify or change NTP servers, it is required that both the NTP server's address type and address be set in the command line simultaneously.

For example, the SNMP command to change the primary NTP server's address from IPv4 (192.168.84.84) to host name looks similar to the following:

```
snmpset -v2c -c private 192.168.84.84
firstNTPServerAddressType = dns firstNTPServerAddress =
"angu.pep.com"
```

Retrieving Energy Usage

You can discover how much energy an IT device consumes by retrieving the Active Energy for the outlet this IT device is plugged into. The Active Energy values are included in the outletSensorMeasurementsTable, along with other outlet sensor readings.

A Note about Enabling Thresholds

When enabling previously disabled thresholds via SNMP, make sure you set a correct value for all thresholds that are supposed to be enabled prior to actually enabling them. Otherwise, you may get an error message.

Chapter 8 Using the Command Line Interface

This section explains how to use the command line interface (CLI) to administer a PX device.

In This Chapter

About the Interface 273
Logging in to CLI 274
Help Command 277
Querying Available Parameters for a Command 278
Showing Information 279
Clearing Information 304
Configuring the PX Device and Network 305
Load Shedding Configuration Commands 437
Power Control Operations 438
Unblocking a User 441
Resetting the PX 442
Network Troubleshooting 442
Retrieving Previous Commands 446
Automatically Completing a Command 446
Logging out of CLI 447

About the Interface

The PX provides a command line interface that enables data center administrators to perform some basic management tasks.

Using this interface, you can do the following:

- Reset the PX device
- Display the PX and network information, such as the device name, firmware version, IP address, and so on
- Configure the PX and network settings
- Troubleshoot network problems

You can access the interface over a local connection using a terminal emulation program such as HyperTerminal, or via a Telnet or SSH client such as PuTTY.

Note: Telnet access is disabled by default because it communicates openly and is thus insecure. To enable Telnet, see **Modifying the Network Service Settings** *(on page 105).*

Logging in to CLI

Logging in via HyperTerminal over a local connection is a little different than logging in using SSH or Telnet.

If a security login agreement has been enabled, you must accept the agreement in order to complete the login. Users are authenticated first and the security banner is checked afterwards.

With HyperTerminal

You can use any terminal emulation programs for local access to the command line interface.

This section illustrates HyperTerminal, which is part of Windows operating systems prior to Windows Vista.

To log in using HyperTerminal:

1. Connect your computer to the PX device via a local connection.
2. Launch HyperTerminal on your computer and open a console window. When the window first opens, it is blank.

   Make sure the COM port settings use this configuration:

   - Bits per second = 115200 (115.2Kbps)
   - Data bits = 8
   - Stop bits = 1
   - Parity = None
   - Flow control = None

   Tip: For a USB connection, you can find out which COM port is assigned to the PX by choosing Control Panel > System > Hardware > Device Manager, and locating the "XXX Serial Console" under the Ports group, where XXX represents this product's name.

3. Press Enter. The Username prompt appears.

   ```
   Username: _
   ```

4. Type a name and press Enter. The name is case sensitive, so make sure you capitalize the correct letters. Then you are prompted to enter a password.

```
Username: admin
Password: _
```

5. Type a password and press Enter. The password is case sensitive, so make sure you capitalize the correct letters.

   After properly entering the password, the # or > system prompt appears. See ***Different CLI Modes and Prompts*** (on page 276) in the PX User Guide for details.

   Tip: The "Last Login" information, including the date and time, is also displayed if the same user profile was once used to log in to the PX web interface or CLI.

6. You are now logged in to the command line interface and can begin administering the PX device.

With SSH or Telnet

You can remotely log in to the command line interface using an SSH or Telnet client, such as PuTTY.

Note: PuTTY is a free program you can download from the Internet. See PuTTY's documentation for details on configuration.

To log in using SSH or Telnet:

1. Ensure SSH or Telnet has been enabled. See ***Modifying the Network Service Settings*** (on page 105) in the PX User Guide.
2. Launch an SSH or Telnet client and open a console window. A login prompt appears.

```
login as:
```

3. Type a name and press Enter. The name is case sensitive, so make sure you capitalize the correct letters.

   Note: If using the SSH client, the name must NOT exceed 25 characters. Otherwise, the login fails.

   Then you are prompted to enter a password.

```
login as: admin
admin@192.168.84.88's password:
```

4. Type a password and press Enter. The password is case sensitive, so make sure you capitalize the correct letters.

5. After properly entering the password, the # or > system prompt appears. See ***Different CLI Modes and Prompts*** (on page 276) in the PX User Guide for details.

   Tip: The "Last Login" information, including the date and time, is also displayed if the same user profile was once used to log in to the PX web interface or CLI.

6. You are now logged in to the command line interface and can begin administering the PX device.

Different CLI Modes and Prompts

Depending on the login name you use and the mode you enter, the system prompt in the CLI varies.

- User Mode: When you log in as a normal user, who may not have full permissions to configure the PX device, the **>** prompt appears.
- Administrator Mode: When you log in as an administrator, who has full permissions to configure the PX device, the # prompt appears.
- Configuration Mode: You can enter the configuration mode from the administrator or user mode. In this mode, the prompt changes to **config:#** or **config:>** and you can change PX device and network configurations. See ***Entering the Configuration Mode*** (on page 305).
- Diagnostic Mode: You can enter the diagnostic mode from the administrator or user mode. In this mode, the prompt changes to **diag:#** or **diag:>** and you can perform the network troubleshooting commands, such as the ping command. See ***Entering the Diagnostic Mode*** (on page 443).

Closing a Local Connection

Close the window or terminal emulation program when you finish accessing a PX device over the local connection.

When accessing or upgrading multiple PX devices, do not transfer the local connection cable from one device to another without closing the local connection window first.

Help Command

The help (?) command shows a list of main CLI commands available for the current mode. This is helpful when you are not familiar with the CLI commands.

- **The help command syntax under the administrator mode is:**

  ```
  #            ?
  ```

- **The help command syntax under the configuration mode is:**

  ```
  config:#     ?
  ```

- **The help command syntax under the diagnostic mode is:**

  ```
  diag:#       ?
  ```

Press Enter after typing the command, and a list of main commands for the current mode is displayed.

Tip: You can check what parameters are available for a specific CLI command by adding the help command to the end of the queried command. See **Querying Available Parameters for a Command** *(on page 278).*

Querying Available Parameters for a Command

If you are not sure what commands or parameters are available for a particular type of CLI command or its syntax, you can have the CLI show them by adding a space and the help command (?) to the end of that command. A list of available parameters and their descriptions will be displayed.

The following shows a few query examples.

- **To query available parameters for the "show" command, the syntax is:**

```
#           show ?
```

- **To query available parameters for the "show user" command, the syntax is:**

```
#           show user ?
```

- **To query available network configuration parameters, the syntax is:**

```
config:#    network ?
```

- **To query available role configuration parameters, the syntax is:**

```
config:#    role ?
```

- **To query available parameters for the "role create" command, the syntax is:**

```
config:#    role create ?
```

Showing Information

You can use the show commands to view current settings or status of the PX device or part of it, such as the IP address, networking mode, firmware version, states or readings of internal or external sensors, user profiles, and so on.

Some "show" commands have two formats: one with the parameter "details" and the other without. The difference is that the command without the parameter "details" displays a shortened version of information while the other displays in-depth information.

After typing a "show" command, press Enter to execute it.

Note: Depending on your login name, the # prompt may be replaced by the > prompt. See **Different CLI Modes and Prompts** *(on page 276).*

Network Configuration

This command shows all network configuration, such as the IP address, networking mode, and MAC address.

```
#       show network
```

IP Configuration

This command shows the IP-related configuration only, such as IPv4 and IPv6 configuration, address(es), gateway, and subnet mask.

```
#       show network ip <option>
```

Variables:

- <option> is one of the options: *all*, *v4* or *v6*.

Option	Description
all	This options shows both of IPv4 and IPv6 settings. *Tip: You can also type the command without adding this option "all" to get the same data.*
v4	This option shows the IPv4 settings only.
v6	This option shows the IPv6 settings only.

LAN Interface Settings

This command shows the LAN interface information only, such as LAN interface speed, duplex mode, and current LAN interface status.

```
#       show network interface
```

Networking Mode

This command shows whether the current networking mode is wired or wireless.

```
#       show network mode
```

Note: If the PX is a slave device connected to the LAN via the master PX device, the `show network mode` *command displays* wired(USB) *instead of* wired*.*

Wireless Configuration

This command only shows the wireless configuration of the PX device, such as the SSID parameter.

```
#       show network wireless
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show network wireless details
```

Network Service Settings

This command shows the network service settings only, including the Telnet setting, TCP ports for HTTP, HTTPS and SSH services, and SNMP settings.

```
#       show network services <option>
```

Variables:

- <option> is one of the options: *all*, *http*, *https*, *telnet*, *ssh*, *snmp* and *zeroconfig*.

Option	Description
all	Displays the settings of all network services, including HTTP, HTTPS, Telnet, SSH and SNMP. *Tip: You can also type the command without adding this option "all" to get the same data.*
http	Only displays the TCP port for the HTTP service.
https	Only displays the TCP port for the HTTPS service.
telnet	Only displays the settings of the Telnet service.
ssh	Only displays the settings of the SSH service.
snmp	Only displays the SNMP settings.
zeroconfig	Only displays the settings of the zero configuration advertising.
modbus	Only displays the settings of the Modbus/TCP service.

PDU Configuration

This command shows the PDU configuration, such as the device name, firmware version and model type.

```
#       show pdu
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show pdu details
```

Outlet Information

This command syntax shows the outlet information.

```
#       show outlets <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show outlets <n> details
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all outlets. *Tip: You can also type the command without adding this option "all" to get the same data.*
A specific outlet number	Displays the information for the specified outlet only.

Displayed information:

- Without the parameter "details," only the outlet state is displayed.
- With the parameter "details," more outlet information is displayed in addition to the state, such as the name, rated current, operating voltage and outlet settings.

Inlet Information

This command syntax shows the inlet information.

```
#       show inlets <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show inlets <n> details
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all inlets. *Tip: You can also type the command without adding this option "all" to get the same data.*
A specific inlet number	Displays the information for the specified inlet only. An inlet number needs to be specified only when there are more than 1 inlet on your PDU.

Displayed information:

- Without the parameter "details," only the inlet's RMS current value(s) and inlet name are displayed.
- With the parameter "details," more inlet information is displayed in addition to the RMS current values, such as the inlet's RMS current, voltage, and active power.

Circuit Breaker Information

This command is only available for PDUs with overcurrent protection mechanism implemented.

This command syntax shows the circuit breaker information.

```
#        show ocp <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#        show ocp <n> details
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all circuit breakers. *Tip: You can also type the command without adding this option "all" to get the same data.*
A specific circuit breaker number	Displays the information for the specified circuit breaker only.

Displayed information:

- Without the parameter "details," only the circuit breaker status and name are displayed.
- With the parameter "details," more circuit breaker information is displayed in addition to status, such as the rating and RMS current value.

Date and Time Settings

This command shows the current date and time settings on the PX device.

```
#        show time
```

To show detailed information, add the parameter "details" to the end of the command.

```
#        show time details
```

Default Measurement Units

This command shows the default measurement units applied to the PX web and CLI interfaces across all users, especially those users authenticated through remote authentication servers.

```
#       show user defaultPreferences
```

Note: If a user has set his/her own preferred measurement units or the administrator has changed any user's preferred units, the web and CLI interfaces show the preferred measurement units for that user instead of the default ones after that user logs in to the PX. See **Existing User Profiles** *(on page 295) for the preferred measurement units for a specific user.*

Environmental Sensor Information

This command syntax shows the environmental sensor's information.

```
#       show externalsensors <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show externalsensors <n> details
```

```
External sensor 3 ('Temperature 1')
Sensor type: Temperature
Reading:     31.8 deg C (normal)

Serial number: AEI0950133
Description:   Not configured
Location:      X Not configured
               Y Not configured
               Z Not configured
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays the information for all environmental sensors. *Tip: You can also type the command without adding this option "all" to get the same data.*
A specific environmental sensor number*	Displays the information for the specified environmental sensor only.

* The environmental sensor number is the ID number assigned to the sensor, which can be found on the External Sensors page of the PX web interface.

Displayed information:

- Without the parameter "details," only the sensor ID, sensor type and reading are displayed.

  Note: A state (on/off) sensor displays the sensor state instead of the numeric reading.

- With the parameter "details," more information is displayed in addition to the ID number and sensor reading, such as the serial number and X, Y, and Z coordinates.

Outlet Sensor Threshold Information

This command syntax shows the specified outlet sensor's threshold-related information.

```
#       show sensor outlet <n> <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show sensor outlet <n> <sensor type> details
```

Variables:

- <n> is the number of the outlet whose sensors you want to query.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor

Displayed information:

- Without the parameter "details," only the sensor reading, state, threshold, deassertion hysteresis and assertion delay settings of the specified outlet sensor are displayed.
- With the parameter "details," more sensor information is displayed, including accuracy and range.
- If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

Outlet Pole Sensor Threshold Information

This command is available for an in-line monitor only (that is, PX2-3nnn series, where n is a number).

This command syntax shows the specified outlet pole sensor's threshold-related information.

```
#       show sensor outletpole <n> <p> <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show sensor outletpole <n> <p> <sensor type> details
```

Variables:

- <n> is the number of the outlet whose pole sensors you want to query.
- <p> is the label of the outlet pole whose sensors you want to query.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 - L2
2	**L2**	L2	L2 - L3
3	**L3**	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor

Sensor type	Description
powerFactor	Power factor sensor
activeEnergy	Active energy sensor

Displayed information:

- Without the parameter "details," only the reading, state, threshold, deassertion hysteresis and assertion delay settings of the specified outlet pole sensor are displayed.
- With the parameter "details," more sensor information is displayed, including accuracy and range.
- If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

Inlet Sensor Threshold Information

This command is not available for an in-line monitor (PX2-3nnn series).

This command syntax shows the specified inlet sensor's threshold-related information.

```
#       show sensor inlet <n> <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show sensor inlet <n> <sensor type> details
```

Variables:

- <n> is the number of the inlet whose sensors you want to query. For a single-inlet PDU, <n> is always the number 1.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Displayed information:

- Without the parameter "details," only the reading, state, threshold, deassertion hysteresis and assertion delay settings of the specified inlet sensor are displayed.
- With the parameter "details," more sensor information is displayed, including accuracy and range.
- If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

Inlet Pole Sensor Threshold Information

This command is only available for a three-phase PDU except for an in-line monitor (PX2-3000 series).

This command syntax shows the specified inlet pole sensor's threshold-related information.

```
#       show sensor inletpole <n> <p> <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show sensor inletpole <n> <p> <sensor type> details
```

Variables:

- <n> is the number of the inlet whose pole sensors you want to query. For a single-inlet PDU, <n> is always the number 1.
- <p> is the label of the inlet pole whose sensors you want to query.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 - L2
2	**L2**	L2	L2 - L3
3	**L3**	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor

Sensor type	Description
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor

Displayed information:

- Without the parameter "details," only the reading, state, threshold, deassertion hysteresis and assertion timeout settings of the specified inlet pole sensor are displayed.
- With the parameter "details," more sensor information is displayed, including accuracy and range.
- If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

Circuit Breaker Sensor Threshold Information

This command is only available for PDUs with overcurrent protection mechanism implemented.

This command syntax shows the specified circuit breaker sensor's threshold-related information.

```
#       show sensor ocp <n> <sensor type>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show sensor ocp <n> <sensor type> details
```

Variables:

- <n> is the number of the circuit breaker whose sensors you want to query.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor

Displayed information:

- Without the parameter "details," only the reading, state, threshold and deassertion hysteresis settings of the specified circuit breaker sensor are displayed.
- With the parameter "details," more sensor information is displayed, including accuracy and range.
- If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

Environmental Sensor Threshold Information

This command syntax shows the specified environmental sensor's threshold-related information.

```
#       show sensor externalsensor <n>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show sensor externalsensor <n> details


External sensor 3 (Temperature):
Reading: 31.8 deg C
State:   normal


Resolution: 0.1 deg C
Accuracy:   +/- 1.00 %
Tolerance:  +/- 0.05 deg C
Range:      -55.0 deg C - 125.0 deg C


Lower critical threshold: 15.0 deg C
Lower warning threshold:  20.0 deg C
Upper warning threshold:  55.0 deg C
Upper critical threshold: 60.0 deg C
Deassertion hysteresis:   1.0 deg C
Assertion timeout:        0 samples
```

Variables:

- <n> is the environmental sensor number. The environmental sensor number is the ID number assigned to the sensor, which can be found on the External Sensors page of the PX web interface.

Displayed information:

- Without the parameter "details," only the reading, threshold, deassertion hysteresis and assertion timeout settings of the specified environmental sensor are displayed.
- With the parameter "details," more sensor information is displayed, including accuracy and range.

Note: For a discrete (on/off) sensor, the threshold-related and accuracy-related data is NOT available.

Security Settings

This command shows the security settings of the PX.

```
#       show security
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show security details
```

Displayed information:

- Without the parameter "details," the information including IP access control, role-based access control, password policy, and HTTPS encryption is displayed.
- With the parameter "details," more security information is displayed, such as user blocking time and user idle timeout.

Existing User Profiles

This command shows the data of one or all existing user profiles.

```
#       show user <user_name>
```

To show detailed information, add the parameter "details" to the end of the command.

```
#       show user <user_name> details
```

Variables:

- <user_name> is the name of the user whose profile you want to query. The variable can be one of the options: *all* or a user's name.

Option	Description
all	This option shows all existing user profiles. *Tip: You can also type the command without adding this option "all" to get the same data.*
a specific user's name	This option shows the profile of the specified user only.

Displayed information:

- Without the parameter "details," only four pieces of user information are displayed: user name, "enabled" status, SNMP v3 access privilege, and role(s).
- With the parameter "details," more user information is displayed, such as the telephone number, e-mail address, preferred measurement units and so on.

Existing Roles

This command shows the data of one or all existing roles.

```
#       show roles <role_name>
```

Variables:

- <role_name> is the name of the role whose permissions you want to query. The variable can be one of the following options:

Option	Description
all	This option shows all existing roles. *Tip: You can also type the command without adding this option "all" to get the same data.*
a specific role's name	This option shows the data of the specified role only.

Displayed information:

- Role settings are displayed, including the role description and privileges.

Load Shedding Settings

This section only applies to outlet-switching capable PDUs.

This command shows the load shedding settings.

```
#       show loadshedding
```

Displayed information:

- The load shedding state is displayed along with non-critical outlets.

Note: The load shedding mode is associated with critical and non-critical outlets. To specify critical and non-critical outlets through CLI, see **Specifying Non-Critical Outlets** *(on page 310).*

Serial Port Settings

This command shows the baud rate setting of the serial port labeled CONSOLE / MODEM on the PX device.

```
#       show serial
```

EnergyWise Settings

This command shows the PX's current configuration for Cisco® EnergyWise.

```
#       show energywise
```

Asset Sensor Settings

This command shows the asset sensor settings, such as the total number of rack units (tag ports), asset sensor state, numbering mode, orientation, available tags and LED color settings.

```
#       show assetStrip <n>
```

Variables:

- <n> is one of the options: *all*, or a number.

Option	Description
all	Displays all asset sensor information. *Tip: You can also type the command without adding this option "all" to get the same data.*
A specific asset sensor number	Displays the settings of the asset sensor connected to the specified FEATURE port number. For the PX device with only one FEATURE port, the valid number is always 1.

Rack Unit Settings of an Asset Sensor

For the Raritan asset sensor, a rack unit refers to a tag port. This command shows the settings of a specific rack unit or all rack units on an asset sensor, such as a rack unit's LED color and LED mode.

```
#       show rackUnit <n> <rack_unit>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the PX device with only one FEATURE port, the number is always 1.
- <rack_unit> is one of the options: *all* or a specific rack unit's index number.

Option	Description
all	Displays the settings of all rack units on the specified asset sensor. *Tip: You can also type the command without adding this option "all" to get the same data.*
A specific number	Displays the settings of the specified rack unit on the specified asset sensor. Use the index number to specify the rack unit. The index number of each rack unit is available on the Asset Strip page of the web interface.

Blade Extension Strip Settings

This command shows the information of a blade extension strip, including the total number of tag ports, and if available, the ID (barcode) number of any connected tag.

```
#       show bladeSlot <n> <rack_unit> <blade_slot>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the PX device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit (tag port) on the selected asset sensor. The index number of each rack unit is available on the Asset Strip page of the web interface.
- <blade_slot> is one of the options: *all* or a specific number of a tag port on the blade extension strip.

Option	Description
all	Displays the information of all tag ports on the specified blade extension strip connected to a particular rack unit. *Tip: You can also type the command without adding this option "all" to get the same data.*
A specific number	Displays the information of the specified tag port on the blade extension strip connected to a particular rack unit. The number of each tag port on the blade extension strip is available on the Asset Strip page.

Event Log

The command used to show the event log begins with `show eventlog`. You can add either the *limit* or *class* parameters or both to show specific events.

- **To show the last 30 entries in the event log:**

```
#       show eventlog
```

- **To show a specific number of last entries in the event log:**

```
#       show eventlog limit <n>
```

- **To show a specific type of events only:**

```
#       show eventlog class <event_type>
```

- ***To show a specific number of last entries associated with a specific type of events only:***

```
#       show eventlog limit <n> class <event_type>
```

Variables:

- <n> is one of the options: *all* or a number.

Option	Description
all	Displays all entries in the event log.
An integer number	Displays the specified number of last entries in the event log. The number ranges between 1 to 10,000.

- <event_type> is one of the following event types.

Event type	Description
all	Displays all types of events.
device	Displays device-related events only, such as system starting or firmware upgrade event.
userAdministration	Displays user management events only, such as creation of a new user profile or a new role.
userActivity	Displays user activities only, such as user login or logout events.
pdu	Displays PDU-related events only, such as entry or exit of the load shedding mode.

Event type	Description
sensor	Only displays events regarding internal or external sensors, such as state changes of any sensors.
serverMonitor	Displays server-monitoring records only. For example, a server being monitored by the PX is declared reachable or unreachable.
energywise	Displays Cisco EnergyWise-related events, such as enabling the support of the EnergyWise function.
assetManagement	Only displays events regarding Raritan's asset management sensor if connected. For example, connection or disconnection of asset management tags.
rfCode	Displays RF Code-related events only, such as connection or disconnection of RF Code tags.
lhx	Only displays events about Schroff® LHX heat exchanger if this device is connected. For example, the fan on the LHX device fails.

Note: You can ignore the powerLogic event type in the CLI because the PX does not support it.

Command History

This command syntax shows the command history for current connection session.

```
#       show history
```

Displayed information:

- A list of commands that were previously entered in the current session is displayed.

History Buffer Length

This command syntax shows the length of the history buffer for storing the history commands.

```
#       show history bufferlength
```

Displayed information:

- The current history buffer length is displayed.

Reliability Data

This command shows the reliability data.

```
#       show reliability data
```

Reliability Error Log

This command shows the reliability error log.

```
#       show reliability errorlog <n>
```

Variables:

- <n> is one of the options: *0* (zero) or any other integer number.

Option	Description
0	Displays all entries in the reliability error log. *Tip: You can also type the command without adding this option "0" to get all data.*
A specific integer number	Displays the specified number of last entries in the reliability error log.

Examples

This section provides examples of the show command.

Example 1 - Basic Security Information

The diagram shows the output of the *show security* command.

```
# show security
IP access control: Disabled

Role based access control: Disabled

Password aging: Enabled

Prevent concurrent user login:   No

Strong passwords: Disabled

Enforce HTTPS for web access: Yes
#
```

Example 2 - In-Depth Security Information

More information is displayed when typing the *show security details* command.

```
# show security details
IP access control: Disabled

Role based access control: Disabled

Password aging: Enabled
Aging interval: 60 days

Prevent concurrent user login:   No
Maximum number of failed logins: 3
User block time:                 10 minutes

User idle timeout: 10 minutes

Strong passwords: Disabled

Enforce HTTPS for web access: Yes
#
```

Example 3 - Basic PDU Information

The diagram shows the output of the *show pdu* command.

```
# show pdu
PDU 'my PX'
Model:            PX2-5260R
Firmware version: 2.2.0.1-26020
#
```

Example 4 - In-Depth PDU Information

More information is displayed when typing the *show pdu details* command.

```
# show pdu details
PDU 'my PX'
Model:            PX2-5260R
Firmware version: 2.2.0.1-26020
Serial number:    PEG1234567

Default outlet state on startup: Last known state
Power cycle delay:               10 seconds

Outlet power sequence:  default
Outlet sequence delays: 1-12: 0 s
Inrush guard delay:     200 ms

Voltage rating:   200-240V
Current rating:   16A
Frequency rating: 50/60Hz
Power rating:     3.2-3.8kVA

Sensor data retrieval:      Enabled
Measurements per log entry: 60

External sensor Z coordinate format: Rack units
Device altitude:                     0 m
#
```

Clearing Information

You can use the clear commands to remove unnecessary data from the PX.

After typing a "clear" command, press Enter to execute it.

Note: Depending on your login name, the # prompt may be replaced by the > prompt. See **Different CLI Modes and Prompts** *(on page 276).*

Clearing Event Log

This command removes all data from the event log.

```
#       clear eventlog
```

After entering the above command, a message appears, prompting you to confirm the operation. Type y to clear the event log or n to abort the operation.

If you type y, a message "Event log was cleared successfully" is displayed after all data in the event log is deleted.

Configuring the PX Device and Network

To configure the PX device or network settings through the CLI, you must log in as the administrator.

Entering the Configuration Mode

You must enter the configuration mode since configuration commands function in the configuration mode only.

To enter the configuration mode:

1. Ensure you have entered the administrator mode and the # prompt is displayed.

   Note: If you enter the configuration mode from the user mode, you may have limited permissions to make configuration changes. See **Different CLI Modes and Prompts** *(on page 276).*

2. Type `config` and press Enter. The config:# prompt appears, indicating that you have entered the configuration mode.

   ```
   config:# _
   ```

3. Now you can type any configuration command and press Enter to change the settings.

Important: To apply new configuration settings, you must issue the "apply" command before closing the terminal emulation program. Closing the program does not save any configuration changes. See *Quitting the Configuration Mode* **(on page 436).**

PDU Configuration Commands

A PDU configuration command begins with *pdu*. You can use the PDU configuration commands to change the settings that apply to the whole PX device.

The commands are case sensitive so ensure you capitalize them correctly.

Changing the PDU Name

This command syntax changes the PX device's name.

```
config:#   pdu name "<name>"
```

Variables:

- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Example

The following command assigns the name "my px12" to the PDU.

```
config:#   pdu name "my px12"
```

Setting the Outlet Power-On Sequence

This section only applies to outlet-switching capable PDUs.

This command syntax sets the outlet power-on sequence when the PDU powers up.

```
config:#   pdu outletSequence <option>
```

Variables:

- <option> is one of the options: *default*, or a comma-separated list of outlet numbers.

Option	Description
default	All outlets are switched ON in the ASCENDING order (from outlet 1 to the final outlet) when the PX device powers up.
A comma-separated list of outlet numbers	All outlets are switched ON in the order you specify using the comma-separated list. The list must include all outlets on the PDU.

Example

The following command causes a 10-outlet PDU to first power on the 8th to 6th outlets and then the rest of outlets in the ascending order after the PDU powers up.

```
config:#    pdu outletSequence 8-6,1-5,9,10
```

Setting the Outlet Power-On Sequence Delay

This section only applies to outlet-switching capable PDUs.

This command syntax sets the delays (in seconds) for outlets when turning on all outlets in sequence.

```
config:#    pdu outletSequenceDelay <outlet1>:<delay1>;<outlet2>:<delay2>;
            <outlet3>:<delay3>;...
```

Separate outlet numbers and their delay settings with a colon. Outlets followed by delays are separated with a semicolon.

Variables:

- <outlet1>, <outlet2>, <outlet3> and the like are individual outlet numbers or a range of outlets.
- <delay1>, <delay2>, <delay3> and the like are the delay time in seconds.

Example

The following command determines that the outlet 1's delay is 2.5 seconds, outlet 2's delay is 3 seconds, and the delay for outlets 3 through 5 is 10 seconds.

```
config:#    pdu outletSequenceDelay 1:2.5;2:3;3-5:10
```

Setting the PDU-Defined Default Outlet State

This section only applies to outlet-switching capable PDUs.

This command syntax determines the initial power condition of all outlets after powering up the PDU.

```
config:#   pdu outletStateOnDeviceStartup <option>
```

Variables:

- <option> is one of the options: *off*, *on* or *lastKnownState*.

Option	Description
off	Switches OFF all outlets when the PX device powers up.
on	Switches ON all outlets when the PX device powers up.
lastKnownState	Restores all outlets to the previous status before powering down the PX device when the PDU powers up again.

Example

The following command causes all outlets to return to the last power state before powering down the PDU, after you power up the PDU again.

```
config:#   pdu outletStateOnDeviceStartup lastKnownState
```

Setting the PDU-Defined Cycling Power-Off Period

This section only applies to outlet-switching capable PDUs.

This command syntax sets the power-off period of the power cycling operation for all outlets.

```
config:#   pdu cyclingPowerOffPeriod <timing>
```

Variables:

- <timing> is the time of the cycling power-off period in seconds, which is an integer between 0 and 3600.

Example

The following command sets the power off period of the power cycling operation to 5 seconds.

```
config:#   pdu cyclingPowerOffPeriod 5
```

Setting the Inrush Guard Delay Time

This section only applies to outlet-switching capable PDUs.

This command syntax sets the inrush guard delay.

```
config:#   pdu inrushGuardDelay <timing>
```

Variables:

- <timing> is a delay time between 100 and 100000 milliseconds.

Example

The following command sets the inrush guard delay to 1000 milliseconds (that is, 1 second).

```
config:#   pdu inrushGuardDelay 1000
```

Setting the Outlet Initialization Delay

This section only applies to outlet-switching capable PDUs.

This command syntax determines the outlet initialization delay timing on device startup. See ***Setting the Initialization Delay*** (on page 164) for information on outlet initialization delay.

```
config:#   pdu outletInitializationDelayOnDeviceStartup <timing>
```

Variables:

- <timing> is a delay time between 1 and 3600 seconds.

Example

The following command sets the outlet initialization delay timing to 5 seconds.

```
config:#   pdu outletInitializationDelayOnDeviceStartup 5
```

Specifying Non-Critical Outlets

This section only applies to outlet-switching capable PDUs.

This command syntax determines critical and non-critical outlets. It is associated with the load shedding mode. See ***Setting Non-Critical Outlets and Load Shedding Mode*** (on page 167).

```
config:#   pdu nonCriticalOutlets <outlets1>:false;<outlets2>:true
```

Separate outlet numbers and their settings with a colon. Separate each "false" and "true" setting with a semicolon.

Variables:

- <outlets1> is one or multiple outlet numbers to be set as critical outlets. Use commas to separate outlet numbers.
- <outlets2> is one or multiple outlet numbers to be set as NON-critical outlets. User commas to separate outlet numbers.

Example

The following command sets outlets 1, 2, 3, 7, and 9 to be critical outlets, and 4, 5, 6, 8, 10, 11 and 12 to be non-critical outlets on a 12-outlet PDU.

```
config:#   pdu nonCriticalOutlets 1-3,7,9:false;4-6,8,10-12:true
```

Enabling or Disabling Data Logging

This command syntax enables or disables the data logging feature.

```
config:#   pdu dataRetrieval <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the data logging feature.
disable	Disables the data logging feature.

For more information, see ***Setting Data Logging*** (on page 116).

Example

The following command enables the data logging feature.

```
config:#   pdu dataRetrieval enable
```

Setting the Data Logging Measurements Per Entry

This command syntax defines the number of measurements accumulated per log entry.

```
config:#   pdu measurementsPerLogEntry <number>
```

Variables:

- <number> is an integer between 1 and 600. The default is 60 samples per log entry.

For more information, see ***Setting Data Logging*** (on page 116).

Example

The following command determines that 66 measurements are accumulated per log entry for sensors, that is, 66 seconds.

```
config:#   pdu measurementsPerLogEntry 66
```

Specifying the Device Altitude

This command syntax specifies your PX device's altitude above sea level (in meters). You must specify the PX device's altitude above sea level if a Raritan differential air pressure sensor is attached. This is because the device's altitude is associated with the altitude correction factor. See ***Altitude Correction Factors*** (on page 499).

```
config:#   pdu deviceAltitude <altitude>
```

Variables:

- <altitude> is an integer between 1 and 3000 meters.

Example

The following command determines that the PX device is located at 1500 meters above sea level.

```
config:#   pdu deviceAltitude 1500
```

Setting the Z Coordinate Format for Environmental Sensors

This command syntax enables or disables the use of rack units for specifying the height (Z coordinate) of environmental sensors.

```
config:#   pdu externalSensorsZCoordinateFormat <option>
```

Variables:

- <option> is one of the options: *rackUnits* or *freeForm*.

Option	Description
rackUnits	The height of the Z coordinate is measured in standard rack units. When this is selected, you can type a numeric value in the rack unit to describe the Z coordinate of any environmental sensors.

Option	Description
freeForm	Any alphanumeric string can be used for specifying the Z coordinate.

Note: After determining the format for the Z coordinate, you can set a value for it. See **Setting the Z Coordinate** *(on page 373).*

Example

The following command determines that the unit of rack is used for specifying the Z coordinate of environmental sensors.

```
config:#   pdu externalSensorsZCoordinateFormat rackUnits
```

Changing the LED Display Orientation

This command syntax determines the orientation of the alphanumeric values shown on the LED display of a *Zero U* PDU.

```
config:#   pdu displayOrientation <orientation>
```

Variables:

- <orientation> is one of the options: *automatic*, *flipped* or *normal*.

Option	Description
automatic	The direction of the values shown on the LED display is determined depending on the PDU's orientation detected by the built-in tilt sensor.
flipped	The values shown on the LED display always stay in the opposite direction regardless of the PDU's orientation.
normal	The values shown on the LED display always stay in the normal direction regardless of the PDU's orientation.

Note that this command is NOT applicable to a non-Zero U PDU.

Example

The following command makes the Zero U PDU reverses the direction of the value shown on the LED display.

```
config:#   pdu displayOrientation flipped
```

Networking Configuration Commands

A network configuration command begins with *network*. A number of network settings can be changed through the CLI, such as the IP address, transmission speed, duplex mode, and so on.

Setting the Networking Mode

If your PX device is implemented with both of the wired and wireless networking mechanisms, you must determine which mechanism is enabled for network connectivity before further configuring networking parameters.

This command syntax enables the wired or wireless networking mode.

```
config:#   network mode <mode>
```

Variables:

- <mode> is one of the modes: *wired* or *wireless*.

Mode	Description
wired	Enables the wired networking mode.
wireless	Enables the wireless networking mode.

Note: If you enable the wireless networking mode, and the PX does not detect any wireless USB LAN adapter or the connected wireless USB LAN adapter is not supported, the message "Supported Wireless device not found" is displayed.

Example

The following command enables the wired networking mode.

```
config:#   network mode wired
```

Configuring IP Protocol Settings

By default, only the IPv4 protocol is enabled. You can enable both the IPv4 and IPv6 protocols, or only the IPv6 protocol for your PX device.

An IP protocol configuration command begins with *network ip*.

Enabling IPv4 or IPv6

This command syntax determines which IP protocol is enabled on the PX.

```
config:#   network ip proto <protocol>
```

Variables:

- <protocol> is one of the options: *v4Only*, *v6Only* or *both*.

Mode	Description
v4Only	Enables IPv4 only on all interfaces. This is the default.
v6Only	Enables IPv6 only on all interfaces.
both	Enables both IPv4 and IPv6 on all interfaces.

Example

The following command determines that both of IPv4 and IPv6 protocols are enabled.

```
config:#   network ip proto both
```

Selecting IPv4 or IPv6 Addresses

This command syntax determines which IP address is used when the DNS server returns both of IPv4 and IPv6 addresses. You need to configure this setting only after both of IPv4 and IPv6 protocols are enabled on the PX.

```
config:#   network ip dnsResolverPreference <resolver>
```

Variables:

- <resolver> is one of the options: *preferV4* or *preferV6.*

Option	Description
preferV4	Use the IPv4 addresses returned by the DNS server.

Option	Description
preferV6	Use the IPv6 addresses returned by the DNS server.

Example

The following command determines that only IPv4 addresses returned by the DNS server are used.

```
config:#   network ip dnsResolverPreference preferV4
```

Setting the Wireless Parameters

You must configure wireless parameters, including Service Set Identifier (SSID), authentication method, Pre-Shared Key (PSK), and Basic Service Set Identifier (BSSID) after the wireless networking mode is enabled.

A wireless configuration command begins with *network wireless*.

Note: If current networking mode is not wireless, the SSID, PSK and BSSID values are not applied until the networking mode is changed to "wireless." In addition, a message appears, indicating that the active network interface is not wireless.

The commands are case sensitive so ensure you capitalize them correctly.

Setting the SSID

This command syntax specifies the SSID string.

```
config:#   network wireless SSID <ssid>
```

Variables:

- <ssid> is the name of the wireless access point, which consists of:
  - Up to 32 ASCII characters
  - No spaces
  - ASCII codes 0x20 ~ 0x7E

Example

The following command assigns "myssid" as the SSID.

```
config:#   network wireless SSID myssid
```

Setting the Authentication Method

This command syntax sets the wireless authentication method to either PSK or Extensible Authentication Protocol (EAP).

```
config:#   network wireless authMethod <method>
```

Variables:

- <method> is one of the authentication methods: *PSK* or *EAP*.

Method	Description
PSK	The wireless authentication method is set to PSK.
EAP	The wireless authentication method is set to EAP.

Example

The following command sets the wireless authentication method to PSK.

```
config:#   network wireless authMethod PSK
```

Setting the PSK

If the Pre-Shared Key (PSK) authentication method is selected, you must assign a PSK passphrase by using this command syntax.

```
config:#   network wireless PSK <psk>
```

Variables:

- <psk> is a string or passphrase that consists of:
  - 8 to 63 characters
  - No spaces
  - ASCII codes 0x20 ~ 0x7E

Example

This command assigns "encryp-key" as the PSK.

```
config:#   network wireless PSK encryp-key
```

Setting the EAP Parameters

When the wireless authentication method is set to EAP, you must configure EAP authentication parameters, including outer authentication, inner authentication, EAP identity, password, and CA certificate.

Setting the Outer Authentication

This command syntax determines the outer authentication protocol for the EAP.

```
config:#   network wireless eapOuterAuthentication <outer_auth>
```

Variables:

- The value of <outer_auth> is *PEAP* because PX only supports Protected Extensible Authentication Protocol (PEAP) as the outer authentication.

Example

The following command determines the outer authentication protocol for the EAP authentication is Protected Extensible Authentication Protocol (PEAP).

```
config:#   network wireless eapOuterAuthentication PEAP
```

Setting the Inner Authentication

This command syntax determines the inner authentication protocol for the EAP.

```
config:#   network wireless eapInnerAuthentication <inner_auth>
```

Variables:

- The value of <inner_auth> is *MSCHAPv2* because PX only supports Microsoft's Challenge Authentication Protocol Version 2 (MSCHAPv2) as the inner authentication.

Example

The following command determines the inner authentication protocol for the EAP authentication is MSCHAPv2.

```
config:#   network wireless eapInnerAuthentication MSCHAPv2
```

Setting the EAP Identity

This command syntax determines the EAP identity.

```
config:#   network wireless eapIdentity <identity>
```

Variables:

- <identity> is your user name for the EAP authentication.

Example

The following command sets the EAP identity to "eap_user01."

```
config:#   network wireless eapIdentity eap_user01
```

Setting the EAP Password

This command syntax determines the EAP password.

```
config:#   network wireless eapPassword
```

Variables:

- <password> is your password for EAP authentication.

Example

The following command sets the EAP password to "user01_password."

```
config:#   network wireless eapPassword user01_password
```

Providing the EAP CA Certificate

You may need to provide a third-party CA certificate for the EAP authentication.

To provide a CA certificate:

1. Type the CA certificate command as shown below and press Enter.

   ```
   config:#   network wireless eapCACertificate
   ```

2. The system prompts you to enter the contents of the CA certificate. Do the following to input the contents:
   a. Open your CA certificate with a text editor.
   b. Copy the contents between the "--- BEGIN CERTIFICATE ---" and "--- END CERTIFICATE ---" lines in a certificate.
   c. Paste the certificate contents into the terminal.
   d. Press Enter.

   Tip: To remove an existing CA certificate, simply press Enter without typing or pasting anything when the system prompts you to input the certificate contents.

3. If the certificate is valid, the system shows the command prompt "`config:#`" again. If not, it shows a message indicating that the certificate is not valid.

Example

This section provides a CA certificate example only. Your CA certificate contents should be different from the contents displayed in this example.

To provide a CA certificate:

1. Make sure you have entered the configuration mode. See ***Entering the Configuration Mode*** (on page 305).
2. Type the following command and press Enter.

   ```
   config:#   network wireless eapCACertificate
   ```

3. The system prompts you to enter the contents of the CA certificate.
4. Open a CA certificate using a text editor. You should see certificate contents similar to the following.

5. Select and copy the contents, excluding the starting line containing "BEGIN CERTIFICATE" and the ending line containing "END CERTIFICATE" as illustrated below.

```
MIICjTCCAfigAwIBAgIEMaYgRzALBgkqhkiG9w0BAQQwRTELMAk
GA1UEBhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aW
NzIGFuZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjAmFxE5NjA1MjgxM
zQ5MDUrMDgwMBcROTgwNTI4MTM0OTA1KzA4MDAwZzELMAkGA1UE
BhMCVVMxNjA0BgNVBAoTLU5hdGlvbmFsIEFlcm9uYXV0aWNzIGF
uZCBTcGFjZSBBZG1pbmlzdHJhdGlvbjEgMAkGA1UEBRMCMTYwEw
YDVQQDEwxTdGV2ZSBTY2hvY2gwWDALBgkqhkiG9w0BAQEDSQAwR
gJBALrAwyYdgxmzNP/ts0Uyf6BpmiJYktU/w4NG67ULaN4B5CnE
z7k57s9o3YY3LecETgQ5iQHmkwlYDTL2fTgVfw0CAQOjgaswgag
wZAYDVR0ZAQH/BFowWDBWMFQxCzAJBgNVBAYTAlVTMTYwNAYDVQ
QKEy1OYXRpb25hbCBBZXJvbmF1dGljcyBhbmQgU3BhY2UgQWRta
W5pc3RyYXRpb24xDTALBgNVBAMTBENSTDEwFwYDVR0BAQH/BA0w
C4AJODMyOTcwODEwMBgGA1UdAgQRMA8ECTgzMjk3MDgyM4ACBSA
wDQYDVR0KBAYwBAMCBkAwCwYJKoZIhvcNAQEEA4GBAH2y1VCEw/
A4zaXzSYZJTTUi3uawbbFiS2yxHvgf28+8Js0OHXk1H1w2d6qOH
H21X82tZXd/0JtG0g1T9usFFBDvYK8O0ebgz/P5ELJnBL2+atOb
EuJy1ZZ0pBDWINR3WkDNLCGiTkCKp0F5EWIrVDwh54NNevkCQRZ
ita+z4IBO
```

6. Paste the contents in the terminal.
7. Press Enter.
8. Verify whether the system shows the following command prompt, indicating the provided CA certificate is valid.

```
config:#
```

Setting the BSSID

This command syntax specifies the BSSID.

```
config:#   network wireless BSSID <bssid>
```

Variables:

- <bssid> is either the MAC address of the wireless access point or *none* if the access point has no MAC address.

Example

The following command specifies that the BSSID is 00:14:6C:7E:43:81.

```
config:#   network wireless BSSID 00:14:6C:7E:43:81
```

Configuring the IPv4 Parameters

An IPv4 configuration command begins with *network ipv4*.

The commands are case sensitive so ensure you capitalize them correctly.

Setting the IPv4 Configuration Mode

This command syntax determines the IP configuration mode.

```
config:#   network ipv4 ipConfigurationMode <mode>
```

Variables:

- <mode> is one of the modes: *dhcp* or *static*.

Mode	Description
dhcp	The IPv4 configuration mode is set to DHCP.
static	The IPv4 configuration mode is set to static IP address.

Example

The following command enables the Static IP configuration mode.

```
config:#   network ipv4 ipConfigurationMode static
```

Setting the IPv4 Preferred Host Name

After selecting DHCP as the IPv4 configuration mode, you can specify the preferred host name, which is optional. The following is the command syntax:

```
config:#   network ipv4 preferredHostName <name>
```

Variables:

- <name> is a host name which:
  - Consists of alphanumeric characters and/or hyphens
  - Cannot begin or end with a hyphen
  - Cannot contain more than 63 characters
  - Cannot contain punctuation marks, spaces, and other symbols

Example

The following command sets the IPv4 preferred host name to "my-v4host."

```
config:#   network ipv4 preferredHostName my-v4host
```

Setting the IPv4 Address

After selecting the static IP configuration mode, you can use this command syntax to assign a permanent IP address to the PX device.

```
config:#   network ipv4 ipAddress <ip address>
```

Variables:

- <ip address> is the IP address being assigned to your PX device. The value ranges from 0.0.0.0 to 255.255.255.255.

Example

The following command assigns the static IPv4 address "192.168.84.222" to the PX device.

```
config:#   network ipv4 ipAddress 192.168.84.222
```

Setting the IPv4 Subnet Mask

After selecting the static IP configuration mode, you can use this command syntax to define the subnet mask.

```
config:#   network ipv4 subnetMask <netmask>
```

Variables:

- <netmask> is the subnet mask address. The value ranges from 0.0.0.0 to 255.255.255.255.

Example

The following command sets the subnet mask to 192.168.84.0.

```
config:#   network ipv4 subnetMask 192.168.84.0
```

Setting the IPv4 Gateway

After selecting the static IP configuration mode, you can use this command syntax to specify the gateway.

```
config:#   network ipv4 gateway <ip address>
```

Variables:

- <ip address> is the IP address of the gateway. The value ranges from 0.0.0.0 to 255.255.255.255.

Example

The following command sets the IPv4 gateway to 255.255.255.0.

```
config:#   network ipv4 gateway 255.255.255.0
```

Setting the IPv4 Primary DNS Server

After selecting the static IP configuration mode, you can use this command syntax to specify the primary DNS server.

```
config:#   network ipv4 primaryDNSServer <ip address>
```

Variables:

- <ip address> is the IP address of the primary DNS server. The value ranges from 0.0.0.0 to 255.255.255.255.

Example

The following command determines that the primary DNS server is 192.168.84.30.

```
config:#   network ipv4 primaryDNSServer 192.168.84.30
```

Setting the IPv4 Secondary DNS Server

After selecting the static IP configuration mode, you can use this command syntax to specify the secondary DNS server.

```
config:#   network ipv4 secondaryDNSServer <ip address>
```

Variables:

- <ip address> is the IP address of the secondary DNS server. The value ranges from 0.0.0.0 to 255.255.255.255.

Note: The PX supports a maximum of 3 DNS servers. If two IPv4 DNS servers and two IPv6 DNS servers are available, the PX only uses the primary IPv4 and IPv6 DNS servers.

Example

The following command determines that the secondary DNS server is 192.168.84.33.

```
config:#   network ipv4 secondaryDNSServer 192.168.84.33
```

Overriding the IPv4 DHCP-Assigned DNS Server

After specifying the primary/secondary DNS server, you can use this command to override the DHCP-assigned DNS server with the one you specified.

```
config:#   network ipv4 overrideDNS <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	This option overrides the DHCP-assigned DNS server with the primary/secondary DNS server you assign.
disable	This option resumes using the DHCP-assigned DNS server.

Example

The following command overrides the DHCP-assigned DNS server with the one you specified.

```
config:#   network ipv4 overrideDNS enable
```

Configuring the IPv6 Parameters

An IPv6 configuration command begins with *network ipv6*.

The commands are case sensitive so ensure you capitalize them correctly.

Setting the IPv6 Configuration Mode

This command syntax determines the IP configuration mode.

```
config:#   network ipv6 ipConfigurationMode <mode>
```

Variables:

- <mode> is one of the modes: *automatic* or *static*.

Mode	Description
automatic	The IPv6 configuration mode is set to automatic.

Mode	Description
static	The IPv6 configuration mode is set to static IP address.

Example

The following command sets the IP configuration mode to the static IP address mode.

```
config:#   network ipv6 ipConfigurationMode static
```

Setting the IPv6 Preferred Host Name

After selecting DHCP as the IPv6 configuration mode, you can specify the preferred host name, which is optional. The following is the command syntax:

```
config:#   network ipv6 preferredHostName <name>
```

Variables:

- <name> is a host name which:
  - Consists of alphanumeric characters and/or hyphens
  - Cannot begin or end with a hyphen
  - Cannot contain more than 63 characters
  - Cannot contain punctuation marks, spaces, and other symbols

Example

The following command sets the IPv6 preferred host name to "my-v6host."

```
config:#   network ipv6 preferredHostName my-v6host
```

Setting the IPv6 Address

After selecting the static IP configuration mode, you can use this command syntax to assign a permanent IP address to the PX device.

```
config:#   network ipv6 ipAddress <ip address>
```

Variables:

- <ip address> is the IP address being assigned to your PX device. This value uses the IPv6 address format.

Example

The following command assigns the static IPv6 address "3210:4179:0:8:0:800:200:417/128" to the PX device.

```
config:#   network ipv6 ipAddress 3210:4179:0:8:0:800:200:417/128
```

Setting the IPv6 Gateway

After selecting the static IP configuration mode, you can use this command syntax to specify the gateway.

```
config:#   network ipv6 gateway <ip address>
```

Variables:

- <ip address> is the IP address of the gateway. This value uses the IPv6 address format.

Example

The following command sets the gateway to 500:0:330:0:4:9:3:2.

```
config:#   network ipv6 gateway 500:0:330:0:4:9:3:2
```

Setting the IPv6 Primary DNS Server

After selecting the static IP configuration mode, you can use this command syntax to specify the primary DNS server. It is required to enable overriding the auto-assigned DNS server before you can specify the DNS servers manually. See ***Overriding the IPv6 DHCP-Assigned DNS Server*** (on page 330).

```
config:#   network ipv6 primaryDNSServer <ip address>
```

Variables:

- <ip address> is the IP address of the primary DNS server. This value uses the IPv6 address format.

Example

The following command determines that the primary DNS server is 2103:288:8201:1::14.

```
config:#   network ipv6 primaryDNSServer 2103:288:8201:1::14
```

Setting the IPv6 Secondary DNS Server

After selecting the static IP configuration mode, you can use this command syntax to specify the secondary DNS server. It is required to enable overriding the auto-assigned DNS server before you can specify the DNS servers manually. See ***Overriding the IPv6 DHCP-Assigned DNS Server*** (on page 330).

```
config:#   network ipv6 secondaryDNSServer <ip address>
```

Variables:

- <ip address> is the IP address of the secondary DNS server. This value uses the IPv6 address format.

Note: The PX supports a maximum of 3 DNS servers. If two IPv4 DNS servers and two IPv6 DNS servers are available, the PX only uses the primary IPv4 and IPv6 DNS servers.

Example

The following command determines that the secondary DNS server is 2103:288:8201:1::700.

```
config:#   network ipv6 secondaryDNSServer 2103:288:8201:1::700
```

Overriding the IPv6 DHCP-Assigned DNS Server

After specifying the primary/secondary DNS server, you can use this command to override the DHCP-assigned DNS server with the one you specified.

```
config:#   network ipv6 overrideDNS <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	This option overrides the DHCP-assigned DNS server with the primary/secondary DNS server you assign.
disable	This option resumes using the DHCP-assigned DNS server.

Example

The following command overrides the DHCP-assigned DNS server with the one you specified.

```
config:#   network ipv6 overrideDNS enable
```

Setting the LAN Interface Parameters

A LAN interface configuration command begins with *network interface*.

The commands are case sensitive so ensure you capitalize them correctly.

Changing the LAN Interface Speed

This command syntax determines the LAN interface speed.

```
config:#   network interface LANInterfaceSpeed <option>
```

Variables:

- <option> is one of the options: *auto*, *10Mbps*, and *100Mbps*.

Option	Description
auto	System determines the optimum LAN speed through auto-negotiation.

Option	Description
10Mbps	The LAN speed is always 10 Mbps.
100Mbps	The LAN speed is always 100 Mbps.

Example

The following command lets the PX determine the optimal LAN interface speed through auto-negotiation.

```
config:#   network interface LANInterfaceSpeed auto
```

Changing the LAN Duplex Mode

This command syntax determines the LAN interface duplex mode.

```
config:#   network interface LANInterfaceDuplexMode <mode>
```

Variables:

- <mode> is one of the modes: *auto*, *half* or *full*.

Option	Description
auto	The PX selects the optimum transmission mode through auto-negotiation.
half	Half duplex: Data is transmitted in one direction (to or from the PX device) at a time.
full	Full duplex: Data is transmitted in both directions simultaneously.

Example

The following command lets the PX determine the optimal transmission mode through auto-negotiation.

```
config:#   network interface LANInterfaceDuplexMode auto
```

Setting the Network Service Parameters

A network service command begins with *network services*.

Changing the HTTP Port

This command syntax changes the HTTP port.

```
config:#   network services http port <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default HTTP port is 80.

Example

The following command sets the HTTP port to 81.

```
config:#   network services http port 81
```

Changing the HTTPS Port

This command syntax changes the HTTPS port.

```
config:#   network services https port <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default HTTPS port is 443.

Example

The following command sets the HTTPS port to 333.

```
config:#   network services https port 333
```

Changing the Telnet Configuration

You can enable or disable the Telnet service, or change its TCP port using the CLI commands.

A Telnet command begins with *network services telnet*.

Enabling or Disabling Telnet

This command syntax enables or disables the Telnet service.

```
config:#   network services telnet enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The Telnet service is enabled.
false	The Telnet service is disabled.

Example

The following command enables the Telnet service.

```
config:#   network services telnet enabled true
```

Changing the Telnet Port

This command syntax changes the Telnet port.

```
config:#   network services telnet port <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default Telnet port is 23.

Example

The following command syntax sets the TCP port for Telnet to 44.

```
config:#   network services telnet port 44
```

Changing the SSH Configuration

You can enable or disable the SSH service, or change its TCP port using the CLI commands.

An SSH command begins with *network services ssh*.

Enabling or Disabling SSH

This command syntax enables or disables the SSH service.

```
config:#   network services ssh enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The SSH service is enabled.
false	The SSH service is disabled.

Example

The following command enables the SSH service.

```
config:#   network services ssh enabled true
```

Changing the SSH Port

This command syntax changes the SSH port.

```
config:#   network services ssh port <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default SSH port is 22.

Example

The following command syntax sets the TCP port for SSH to 555.

```
config:#   network services ssh port 555
```

Setting the SNMP Configuration

You can enable or disable the SNMP v1/v2c or v3 agent, configure the read and write community strings, or set the MIB-II parameters, such as sysContact, using the CLI commands.

An SNMP command begins with *network services snmp*.

Enabling or Disabling SNMP v1/v2c

This command syntax enables or disables the SNMP v1/v2c protocol.

```
config:#   network services snmp v1/v2c <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	The SNMP v1/v2c protocol is enabled.
disable	The SNMP v1/v2c protocol is disabled.

Example

The following command enables the SNMP v1/v2c protocol.

```
config:#   network services snmp v1/v2c enable
```

Enabling or Disabling SNMP v3

This command syntax enables or disables the SNMP v3 protocol.

```
config:#   network services snmp v3 <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	The SNMP v3 protocol is enabled.
disable	The SNMP v3 protocol is disabled.

Example

The following command enables the SNMP v3 protocol.

```
config:#   network services snmp v3 enable
```

Setting the SNMP Read Community

This command syntax sets the SNMP read-only community string.

```
config:#   network services snmp readCommunity <string>
```

Variables:

- <string> is a string comprising 4 to 64 ASCII printable characters.
- The string CANNOT include spaces.

Example

This command syntax sets the SNMP read-only community string to "public."

```
config:#   network services snmp readCommunity public
```

Setting the SNMP Write Community

This command syntax sets the SNMP read/write community string.

```
config:#   network services snmp writeCommunity <string>
```

Variables:

- <string> is a string comprising 4 to 64 ASCII printable characters.
- The string CANNOT include spaces.

Example

The following command sets the SNMP read/write community string to "private."

```
config:#   network services snmp writeCommunity private
```

Setting the sysContact Value

This command syntax sets the SNMP MIB-II sysContact value.

```
config:#   network services snmp sysContact <value>
```

Variables:

- <value> is a string comprising 0 to 255 alphanumeric characters.

Example

The following command sets the SNMP MIB-II sysContact to "John_Krause."

```
config:#   network services snmp sysContact John_Krause
```

Setting the sysName Value

This command syntax sets the SNMP MIB-II sysName value.

```
config:#   network services snmp sysName <value>
```

Variables:

- <value> is a string comprising 0 to 255 alphanumeric characters.

Example

The following command sets the SNMP MIB-II sysName to "Win7_system"

```
config:#   network services snmp sysName Win7_system
```

Setting the sysLocation Value

This command syntax sets the SNMP MIB-II sysLocation value.

```
config:#   network services snmp sysLocation <value>
```

Variables:

- <value> is a string comprising 0 to 255 alphanumeric characters.

Example

The following command sets the SNMP MIB-II sysLocation to "New_TAIPEI"

```
config:#   network services snmp sysLocation New_TAIPEI
```

Changing the Modbus Configuration

You can enable or disable the Modbus agent, configure its read-only capability, or change its TCP port.

A Modbus command begins with *network services modbus*.

Enabling or Disabling Modbus

This command syntax enables or disables the Modbus protocol.

```
config:#   network services modbus enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The Modbus agent is enabled.
false	The Modbus agent is disabled.

Example

The following command enables the Modbus protocol.

```
config:#   network services modbus enabled true
```

Enabling or Disabling the Read-Only Mode

This command syntax enables or disables the read-only mode for the Modbus agent.

```
config:#   network services modbus readonly <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The read-only mode is enabled.
false	The read-only mode is disabled.

Example

The following command disables the read-only mode for the Modbus agent.

```
config:#   network services modbus readonly false
```

Changing the Modbus Port

This command syntax changes the Modbus port.

```
config:#   network services modbus port <n>
```

Variables:

- <n> is a TCP port number between 1 and 65535. The default Modbus port is 502.

Example

This following command changes the Modbus port.

```
config:#   network services modbus port 600
```

Enabling or Disabling the Service Advertisement

This command syntax enables or disables the zero configuration protocol, which enables advertising or auto discovery of network services. See ***Enabling Service Advertisement*** (on page 109) for details.

```
config:#   network services zeroconfig enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The zero configuration protocol is enabled.
false	The zero configuration protocol is disabled.

Example

The following command enables the zero configuration protocol.

```
config:#   network services zeroconfig enabled true
```

Time Configuration Commands

A time configuration command begins with *time*.

Determining the Time Setup Method

This command syntax determines the method to configure the system date and time.

```
config:#   time method <method>
```

Variables:

- <method> is one of the time setup options: *manual* or *ntp*.

Mode	Description
manual	The date and time settings are customized.
ntp	The date and time settings synchronize with a specified NTP server.

Example

The following command sets the date and time settings by using the NTP servers.

```
config:#   time method ntp
```

Setting the NTP Parameters

A time configuration command that is used to set the NTP parameters begins with *time ntp*.

Specifying the Primary NTP Server

This command syntax specifies the primary time server if synchronization with the NTP server is enabled.

```
config:#   time ntp firstServer <first_server>
```

Variables:

- The <first_server> is the IP address or host name of the primary NTP server.

Example

The following command sets the primary time server to 192.168.80.66.

```
config:#   time ntp firstServer 192.168.80.66
```

Specifying the Secondary NTP Server

This command syntax specifies the primary time server if synchronization with the NTP server is enabled.

```
config:#   time ntp secondServer <second_server>
```

Variables:

- The <second_server> is the IP address or host name of the secondary NTP server.

Example

The following command sets the secondary time server to 192.168.80.78.

```
config:#   time ntp secondServer 192.168.80.78
```

Overriding the DHCP-Assigned NTP Servers

This command syntax determines whether the customized NTP server settings override the DHCP-specified NTP servers.

```
config:#   time ntp overrideDHCPProvidedServer <option>
```

Variables:

- <option> is one of these options: *true* or *false*.

Mode	Description
true	Customized NTP server settings override the DHCP-specified NTP servers.
false	Customized NTP server settings do NOT override the DHCP-specified NTP servers.

Example

The following command overrides the DHCP-specified NTP servers with the customized NTP servers, including the primary and secondary NTP servers.

```
config:#   time ntp overrideDHCPProvidedServer true
```

Setting the Time Zone

In addition to the web interface, the CLI also provides a list of time zones for you to configure the date and time for your PX device.

```
config:#   time zone
```

Example

To set the time zone:

1. Type the time zone command as shown below and press Enter.

   ```
   config:#   time zone
   ```

2. The system shows a list of time zones. Type the index number of the desired time zone and press Enter.
3. Type `apply` for the selected time zone to take effect.

Setting the Automatic Daylight Savings Time

This command syntax enables or disables the application of the daylight savings time to the time settings.

```
config:#   time autoDST <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Mode	Description
enable	Daylight savings time is enabled.
disable	Daylight savings time is disabled.

Example

The following command enables the daylight savings time.

```
config:#   time autoDST enable
```

Security Configuration Commands

A security configuration command begins with *security*.

Firewall Control

You can manage firewall control features through the CLI. The firewall control lets you set up rules that permit or disallow access to the PX device from a specific or a range of IP addresses.

- An IPv4 firewall configuration command begins with *security ipAccessControl ipv4*.
- An IPv6 firewall configuration command begins with *security ipAccessControl ipv6*.

Modifying the Firewall Control Parameters

There are different commands for modifying firewall control parameters.

- **IPv4 commands**

To enable or disable the IPv4 firewall control feature, use this command syntax:

```
config:#   security ipAccessControl ipv4 enabled <option>
```

To determine the default IPv4 firewall control policy, use this command syntax:

```
config:#   security ipAccessControl ipv4 defaultPolicy <policy>
```

- **IPv6 commands**

To enable or disable the IPv6 firewall control feature, use this command syntax:

```
config:#   security ipAccessControl ipv6 enabled <option>
```

To determine the default IPv6 firewall control policy, use this command syntax:

```
config:#   security ipAccessControl ipv6 defaultPolicy <policy>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the IP access control feature.
false	Disables the IP access control feature.

- <policy> is one of the options: *accept, drop* or *reject*.

Option	Description
accept	Accepts traffic from all IP addresses.
drop	Discards traffic from all IP addresses, without sending any failure notification to the source host.

Option	Description
reject	Discards traffic from all IP addresses, and an ICMP message is sent to the source host for failure notification.

Tip: You can combine both commands to modify all firewall control parameters at a time. See **Multi-Command Syntax** *(on page 435).*

Example

The following command sets up two parameters of the IPv4 access control feature.

```
config:#   security ipAccessControl ipv4 enabled true defaultPolicy accept
```

Results:

- The IPv4 access control feature is enabled.
- The default policy is set to "accept."

Managing Firewall Rules

You can add, delete or modify firewall rules using the CLI commands.

- An IPv4 firewall control rule command begins with *security ipAccessControl ipv4 rule*.
- An IPv6 firewall control rule command begins with *security ipAccessControl ipv6 rule*.

Adding a Firewall Rule

Depending on where you want to add a new firewall rule in the list, the command syntax for adding a rule varies.

- **IPv4 commands**

▶ **To add a new rule to the bottom of the IPv4 rules list, use this command syntax:**

```
config:#   security ipAccessControl ipv4 rule add <ip_mask> <policy>
```

▶ **To add a new IPv4 rule by inserting it above or below a specific rule, use this command syntax:**

```
config:#    security ipAccessControl ipv4 rule add <ip_mask> <policy> <insert>
            <rule_number>

            -- OR --

config:#    security ipAccessControl ipv4 rule add <insert> <rule_number> <ip_mask>
            <policy>
```

- **IPv6 commands**

▶ **To add a new rule to the bottom of the IPv6 rules list, use this command syntax:**

```
config:#    security ipAccessControl ipv6 rule add <ip_mask> <policy>
```

▶ **To add a new IPv6 rule by inserting it above or below a specific rule, use this command syntax:**

```
config:#    security ipAccessControl ipv6 rule add <ip_mask> <policy> <insert>
            <rule_number>

            -- OR --

config:#    security ipAccessControl ipv6 rule add <insert> <rule_number> <ip_mask>
            <policy>
```

Variables:

- <ip_mask> is the combination of the IP address and subnet mask values, which are separated with a slash. For example, an IPv4 combination looks like this: *192.168.94.222/24*.
- <policy> is one of the options: *accept, drop* or *reject*.

Policy	Description
accept	Accepts traffic from the specified IP address(es).
drop	Discards traffic from the specified IP address(es), without sending any failure notification to the source host.
reject	Discards traffic from the specified IP address(es), and an ICMP message is sent to the source host for failure notification.

- <insert> is one of the options: *insertAbove* or *insertBelow*.

Option	Description
insertAbove	Inserts the new rule above the specified rule number. Then: new rule's number = the specified rule number
insertBelow	Inserts the new rule below the specified rule number. Then: new rule's number = the specified rule number + 1

- <rule_number> is the number of the existing rule which you want to insert the new rule above or below.

Example

The following command adds a new IPv4 access control rule and specifies its location in the list.

```
config:#   security ipAccessControl ipv4 rule add 192.168.84.123/24 accept
           insertAbove 5
```

Results:

- A new IPv4 firewall control rule is added, allowing all packets from the IPv4 address 192.168.84.123 to be accepted.
- The newly-added rule is inserted above the 5th rule. That is, the new rule becomes the 5th rule, and the original 5th rule becomes the 6th rule.

Modifying a Firewall Rule

Depending on what to modify in an existing rule, the command syntax varies.

- **IPv4 commands**

▶ **The command syntax to modify an IPv4 rule's IP address and/or subnet mask:**

```
config:#   security ipAccessControl ipv4 rule modify <rule_number> ipMask
           <ip_mask>
```

▶ **The command syntax to modify an IPv4 rule's policy:**

```
config:#    security ipAccessControl ipv4 rule modify <rule_number> policy
            <policy>
```

The command syntax to modify all contents of an existing IPv4 rule:

```
config:#    security ipAccessControl ipv4 rule modify <rule_number> ipMask
            <ip_mask> policy <policy>
```

- **IPv6 commands**

The command syntax to modify an IPv6 rule's IP address and/or subnet mask:

```
config:#    security ipAccessControl ipv6 rule modify <rule_number> ipMask
            <ip_mask>
```

The command syntax to modify an IPv6 rule's policy:

```
config:#    security ipAccessControl ipv6 rule modify <rule_number> policy
            <policy>
```

The command syntax to modify all contents of an IPv6 existing rule:

```
config:#    security ipAccessControl ipv6 rule modify <rule_number> ipMask <ip_mask>
            policy <policy>
```

Variables:

- <rule_number> is the number of the existing rule that you want to modify.
- <ip_mask> is the combination of the IP address and subnet mask values, which are separated with a slash. For example, an IPv4 combination looks like this: *192.168.94.222/24*.
- <policy> is one of the options: *accept, drop* or *reject*.

Option	Description
accept	Accepts traffic from the specified IP address(es).

Option	Description
drop	Discards traffic from the specified IP address(es), without sending any failure notification to the source host.
reject	Discards traffic from the specified IP address(es), and an ICMP message is sent to the source host for failure notification.

Example

The following command modifies all contents of the 5th IPv4 rule.

```
config:#   security ipAccessControl ipv4 rule modify 5 ipMask 192.168.84.123/24
           policy accept
```

Results:

- The IPv4 address is changed to 192.168.84.123, and the subnet mask to 255.255.255.0.
- The policy now becomes "accept."

Deleting a Firewall Rule

The following commands remove a specific IPv4 or IPv6 rule from the list.

- **IPv4 commands**

```
config:#   security ipAccessControl ipv4 rule delete <rule_number>
```

- **IPv6 commands**

```
config:#   security ipAccessControl ipv6 rule delete <rule_number>
```

Variables:

- <rule_number> is the number of the existing rule that you want to remove.

Example

The following command removes the 5th rule from the IPv6 access control list.

```
config:#   security ipAccessControl ipv6 rule delete 5
```

Restricted Service Agreement

The CLI command used to set the Restricted Service Agreement feature begin with `security restrictedServiceAgreement`,

Enabling or Disabling the Restricted Service Agreement

This command syntax activates or deactivates the Restricted Service Agreement.

```
config:#   security restrictedServiceAgreement enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the Restricted Service Agreement feature.
false	Disables the Restricted Service Agreement feature.

If the Restricted Service Agreement feature is enabled, the Restricted Service Agreement is displayed when any user logs in to the PX. Do either of the following, or you cannot successfully log in to the PX:

- In the web interface, select the checkbox labeled "I understand and accept the Restricted Service Agreement."
- In the CLI, type y when the confirmation message "I understand and accept the Restricted Service Agreement" is displayed.

Example

The following command disables the Restricted Service Agreement feature.

```
config:#   security restrictedServiceAgreement enabled false
```

Specifying the Agreement Content

This command syntax allows you to create or modify the content for the Restricted Service Agreement.

```
config:#   security restrictedServiceAgreement bannerContent
```

After performing the above command, do the following:

1. Type the text comprising up to 10,000 ASCII characters when the PX CLI prompts you to enter the content.
2. To end the content:
   a. Press Enter.
   b. Type `--END--` to indicate the end of the content.
   c. Press Enter again.

If the content is successfully entered, the CLI displays this message "Successfully entered Restricted Service Agreement" followed by the total number of entered characters in parentheses.

Note: The new content of Restricted Service Agreement is saved only after typing the `apply` command. See **Quitting the Configuration Mode** *(on page 436).*

Example

The following example illustrates how to specify the content of the Restricted Service Agreement.

1. Type the following command and press Enter to start entering the content.

   ```
   config:#   security restrictedServiceAgreement bannerContent
   ```

2. Type the following content when the CLI prompts you to enter the content.

   ```
   IMPORTANT!! You are accessing a PDU. If you are not the
   system administrator, do NOT power off or power cycle
   any outlet without the permission of the system
   administrator.
   ```

3. Press Enter.
4. Type the following:

   ```
   --END--
   ```

5. Press Enter again.
6. Verify that the message "Successfully entered Restricted Service Agreement" is displayed, indicating that the content input is successful.

HTTPS Access

This command determines whether the HTTPS access to the PX web interface is forced. If yes, all HTTP access attempts are automatically directed to HTTPS.

```
config:#   security enforceHttpsForWebAccess <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the HTTPS access to the web interface.
disable	Disables the HTTPS access to the web interface.

Example

The following command disables the HTTPS access feature.

```
config:#   security enforceHttpsForWebAccess disable
```

Login Limitation

The login limitation feature controls login-related limitations, such as password aging, simultaneous logins using the same user name, and the idle time permitted before being forced to log out.

A login limitation command begins with *security loginLimits*.

You can combine multiple commands to modify the login limitation parameters at a time. See ***Multi-Command Syntax*** (on page 435).

Single Login Limitation

This command syntax enables or disables the single login feature, which controls whether multiple logins using the same login name simultaneously is permitted.

```
config:#   security loginLimits singleLogin <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the single login feature.
disable	Disables the single login feature.

Example

The following command disables the single login feature so that more than one user can log in using the same user name at the same time.

```
config:#   security loginLimits singleLogin disable
```

Password Aging

This command syntax enables or disables the password aging feature, which controls whether the password should be changed at a regular interval:

```
config:#   security loginLimits passwordAging <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the password aging feature.
disable	Disables the password aging feature.

Example

The following command enables the password aging feature.

```
config:#   security loginLimits passwordAging enable
```

Password Aging Interval

This command syntax determines how often the password should be changed.

```
config:#   security loginLimits passwordAgingInterval <value>
```

Variables:

- <value> is a numeric value in days set for the password aging interval. The interval ranges from 7 to 365 days.

Example

The following command sets the password again interval to 90 days.

```
config:#   security loginLimits passwordAgingInterval 90
```

Idle Timeout

This command syntax determines how long a user can remain idle before that user is forced to log out of the PX web interface.

```
config:#   security loginLimits idleTimeout <value>
```

Variables:

- <value> is a numeric value in minutes set for the idle timeout. The timeout ranges from 1 to 1440 minutes (24 hours).

Example

The following command sets the idle timeout to 10 minutes.

```
config:#   security loginLimits idleTimeout 10
```

User Blocking

There are different commands for changing different user blocking parameters. These commands begin with `security userBlocking`.

To determine the maximum number of failed logins before blocking a user, use this command syntax:

```
config:#   security userBlocking maximumNumberOfFailedLogins <value1>
```

To determine how long a user's login is blocked, use this command syntax:

```
config:#   security userBlocking blockTime <value2>
```

Variables:

- <value1> is an integer between 3 and 10, or *unlimited*, which sets no limit on the maximum number of failed logins and thus disables the user blocking function.
- <value2> is a numeric value in minutes.

Tip: You can combine multiple commands to modify the user blocking parameters at a time. See **Multi-Command Syntax** *(on page 435).*

Example

The following command sets up two user blocking parameters.

```
config:#   security userBlocking maximumNumberOfFailedLogins 5 blockTime 30
```

Results:

- The maximum number of failed logins is set to 5.
- The user blocking time is set to 30 minutes.

Strong Passwords

The strong password commands determine whether a strong password is required for login, and what a strong password should contain at least.

A strong password command begins with `security strongPasswords`.

You can combine multiple strong password commands to modify different parameters at a time. See ***Multi-Command Syntax*** (on page 435).

Enabling or Disabling Strong Passwords

This command syntax enables or disables the strong password feature.

```
config:#   security strongPasswords enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the strong password feature.
false	Disables the strong password feature.

Example

This command syntax enables the strong password feature.

```
config:#   security strongPasswords enabled true
```

Minimum Password Length

This command syntax determines the minimum length of the password.

```
config:#   security strongPasswords minimumLength <value>
```

Variables:

- <value> is an integer between 8 and 32.

Example

This command syntax determines a password must comprise at least 8 characters.

```
config:#   security strongPasswords minimumLength 8
```

Maximum Password Length

This command syntax determines the maximum length of the password.

```
config:#   security strongPasswords maximumLength <value>
```

Variables:

- <value> is an integer between 16 and 64.

Example

This command syntax determines that a password must NOT comprise more than 20 characters.

```
config:#   security strongPasswords maximumLength 20
```

Lowercase Character Requirement

This command syntax determines whether a strong password includes at least a lowercase character.

```
config:#   security strongPasswords enforceAtLeastOneLowerCaseCharacter <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one lowercase character is required.
disable	No lowercase character is required.

Example

This command syntax determines that a password must include at least a lowercase character.

```
config:#   security strongPasswords enforceAtLeastOneLowerCaseCharacter enable
```

Uppercase Character Requirement

This command syntax determines whether a strong password includes at least a uppercase character.

```
config:#    security strongPasswords enforceAtLeastOneUpperCaseCharacter <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one uppercase character is required.
disable	No uppercase character is required.

Example

This command determines a password must comprise at least one uppercase character.

```
config:#    security strongPasswords enforceAtLeastOneUpperCaseCharacter enable
```

Numeric Character Requirement

This command syntax determines whether a strong password includes at least a numeric character.

```
config:#    security strongPasswords enforceAtLeastOneNumericCharacter <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one numeric character is required.
disable	No numeric character is required.

Example

The following command determines that a password must comprise at least one numeric character.

```
config:#    security strongPasswords enforceAtLeastOneNumericCharacter enable
```

Special Character Requirement

This command syntax determines whether a strong password includes at least a special character.

```
config:#   security strongPasswords enforceAtLeastOneSpecialCharacter <option>
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	At least one special character is required.
disable	No special character is required.

Example

The following command determines that a password must comprise at least one special character.

```
config:#   security strongPasswords enforceAtLeastOneSpecialCharacter enable
```

Maximum Password History

This command syntax determines the number of previous passwords that CANNOT be repeated when changing the password.

```
config:#   security strongPasswords passwordHistoryDepth <value>
```

Variables:

- <value> is an integer between 1 and 12.

Example

The following command determines that the previous 7 passwords CANNOT be re-used when changing the password.

```
config:#   security strongPasswords passwordHistoryDepth 7
```

Role-Based Access Control

In addition to firewall access control based on IP addresses, you can configure other access control rules that are based on both IP addresses and users' roles.

- An IPv4 role-based access control command begins with *security roleBasedAccessControl ipv4*.
- An IPv6 role-based access control command begins with *security roleBasedAccessControl ipv6*.

Modifying the Role-Based Access Control Parameters

There are different commands for modifying role-based access control parameters.

- **IPv4 commands**

▶ **To enable or disable the IPv4 role-based access control feature, use this command syntax:**

```
config:#   security roleBasedAccessControl ipv4 enabled <option>
```

▶ **To determine the IPv4 role-based access control policy, use this command syntax:**

```
config:#   security roleBasedAccessControl ipv4 defaultPolicy <policy>
```

- **IPv6 commands**

▶ **To enable or disable the IPv6 role-based access control feature, use this command syntax:**

```
config:#   security roleBasedAccessControl ipv6 enabled <option>
```

▶ **To determine the IPv6 role-based access control policy, use this command syntax:**

```
config:#   security roleBasedAccessControl ipv6 defaultPolicy <policy>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the role-based access control feature.
false	Disables the role-based access control feature.

- <policy> is one of the options: *allow* or *deny*.

Policy	Description
allow	Accepts traffic from all IP addresses regardless of the user's role.
deny	Drops traffic from all IP addresses regardless of the user's role.

Tip: You can combine both commands to modify all role-based access control parameters at a time. See **Multi-Command Syntax** *(on page 435).*

Example

The following command sets two parameters of the role-based IPv4 access control feature.

```
config:#   security roleBasedAccessControl ipv4 enabled true defaultPolicy allow
```

Results:

- The role-based IPv4 access control feature is enabled.
- The default policy is set to "allow."

Managing Role-Based Access Control Rules

You can add, delete or modify role-based access control rules.

- An IPv4 role-based access control command for managing rules begins with *security roleBasedAccessControl ipv4 rule*.
- An IPv6 role-based access control command for managing rules begins with *security roleBasedAccessControl ipv6 rule*.

Adding a Role-Based Access Control Rule

Depending on where you want to add a new rule in the list, the command syntax for adding a rule varies.

- **IPv4 commands**

▶ **To add a new rule to the bottom of the IPv4 rules list, use this command syntax:**

```
config:#  security roleBasedAccessControl ipv4 rule add <start_ip> <end_ip> <role>
          <policy>
```

▶ **To add a new IPv4 rule by inserting it above or below a specific rule, use this command syntax:**

```
config:#  security roleBasedAccessControl ipv4 rule add <start_ip> <end_ip> <role>
          <policy> <insert> <rule_number>
```

- **IPv6 commands**

▶ **To add a new rule to the bottom of the IPv6 rules list, use this command syntax:**

```
config:#  security roleBasedAccessControl ipv6 rule add <start_ip> <end_ip> <role>
          <policy>
```

▶ **To add a new IPv6 rule by inserting it above or below a specific rule, use this command syntax:**

```
config:#  security roleBasedAccessControl ipv6 rule add <start_ip> <end_ip> <role>
          <policy> <insert> <rule_number>
```

Variables:

- <start_ip> is the starting IP address.
- <end_ip> is the ending IP address.
- <role> is the role for which you want to create an access control rule.
- <policy> is one of the options: *allow* or *deny*.

Policy	Description
allow	Accepts traffic from the specified IP address range when the user is a member of the specified role

Policy	Description
deny	Drops traffic from the specified IP address range when the user is a member of the specified role

- <insert> is one of the options: *insertAbove* or *insertBelow*.

Option	Description
insertAbove	Inserts the new rule above the specified rule number. Then: new rule's number = the specified rule number
insertBelow	Inserts the new rule below the specified rule number. Then: new rule's number = the specified rule number + 1

- <rule_number> is the number of the existing rule which you want to insert the new rule above or below.

Example

The following command creates a newIPv4 role-based access control rule and specifies its location in the list.

```
config:#  security roleBasedAccessControl ipv4 rule add 192.168.78.50 192.168.90.100
          admin deny insertAbove 3
```

Results:

- A new IPv4 role-based access control rule is added, dropping all packets from any IPv4 address between 192.168.78.50 and 192.168.90.100 when the user is a member of the role "admin."
- The newly-added IPv4 rule is inserted above the 3rd rule. That is, the new rule becomes the 3rd rule, and the original 3rd rule becomes the 4th rule.

Modifying a Role-Based Access Control Rule

Depending on what to modify in an existing rule, the command syntax varies.

- **IPv4 commands**

▶ **To modify a rule's IPv4 address range, use this command syntax:**

```
config:#    security roleBasedAccessControl ipv4 rule modify <rule_number>
            startIpAddress <start_ip> endIpAddress <end_ip>
```

- **To modify an IPv4 rule's role, use this command syntax:**

```
config:#    security roleBasedAccessControl ipv4 rule modify <rule_number> role
            <role>
```

- **To modify an IPv4 rule's policy, use this command syntax:**

```
config:#    security roleBasedAccessControl ipv4 rule modify <rule_number> policy
            <policy>
```

- **To modify all contents of an existing IPv4 rule, use this command syntax:**

```
config:#    security roleBasedAccessControl ipv4 rule modify <rule_number>
            startIpAddress <start_ip> endIpAddress <end_ip> role <role> policy
            <policy>
```

- **IPv6 commands**

- **To modify a rule's IPv6 address range, use this command syntax:**

```
config:#    security roleBasedAccessControl ipv6 rule modify <rule_number>
            startIpAddress <start_ip> endIpAddress <end_ip>
```

- **To modify an IPv6 rule's role, use this command syntax:**

```
config:#    security roleBasedAccessControl ipv6 rule modify <rule_number> role
            <role>
```

- **To modify an IPv6 rule's policy, use this command syntax:**

```
config:#    security roleBasedAccessControl ipv6 rule modify <rule_number> policy
            <policy>
```

To modify all contents of an existing IPv6 rule, use this command syntax:

```
config:#    security roleBasedAccessControl ipv6 rule modify <rule_number>
            startIpAddress <start_ip> endIpAddress <end_ip> role <role> policy
            <policy>
```

Variables:

- <rule_number> is the number of the existing rule that you want to modify.
- <start_ip> is the starting IP address.
- <end_ip> is the ending IP address.
- <role> is one of the existing roles.
- <policy> is one of the options: *allow* or *deny*.

Policy	Description
allow	Accepts traffic from the specified IP address range when the user is a member of the specified role
deny	Drops traffic from the specified IP address range when the user is a member of the specified role

Example

The following command modifies all contents of the 8th IPv4 rule.

```
config:#    security roleBasedAccessControl ipv4 rule modify 8
            startIpAddress 192.168.8.8 endIpAddress 192.168.90.90 role operator
            policy allow
```

Results:

- The starting IPv4 address is changed to 192.168.8.8, and the ending IPv4 address to 192.168.90.90.
- The role is changed to "operator."
- The policy now becomes "allow."

Deleting a Role-Based Access Control Rule

This command removes a specific rule from the list.

- **IPv4 commands**

```
config:#   security roleBasedAccessControl ipv4 rule delete <rule_number>
```

- **IPv6 commands**

```
config:#   security roleBasedAccessControl ipv6 rule delete <rule_number>
```

Variables:

- <rule_number> is the number of the existing rule that you want to remove.

Example

The following command removes the 7th IPv6 rule.

```
config:#   security roleBasedAccessControl ipv6 rule delete 7
```

Outlet Configuration Commands

An outlet configuration command begins with *outlet*. Such a command allows you to configure an individual outlet.

Changing the Outlet Name

This command syntax names an outlet.

```
config:#   outlet <n> name "<name>"
```

Variables:

- <n> is the number of the outlet that you want to configure.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Example

The following command assigns the name "Win XP" to outlet 8.

```
config:#   outlet 8 name "Win XP"
```

Changing an Outlet's Default State

This section only applies to outlet-switching capable PDUs.

This command syntax determines the initial power condition of an outlet after the PDU powers up.

```
config:#   outlet <n> stateOnDeviceStartup <option>
```

Variables:

- <n> is the number of the outlet that you want to configure.
- <option> is one of the options: *off*, *on, lastKnownState* and *pduDefined.*

Option	Description
off	Switches OFF the outlet when the PX device powers up.
on	Switches ON the outlet when the PX device powers up.
lastKnownState	Restores the outlet to the previous status before the PX device powered down when powering up the PDU.
pduDefined	Determines the outlet's default state according to the PDU-defined setting.

Note: Setting the outlet's default state to an option other than pduDefined *overrides the PDU-defined default state on that outlet. See* **Setting the PDU-Defined Default Outlet State** *(on page 308).*

Example

The following command makes the outlet 8 return to the last power state before powering down the PDU, after you power it up again.

```
config:#   outlet 8 stateOnDeviceStartup lastKnownState
```

Setting an Outlet's Cycling Power-Off Period

This section only applies to outlet-switching capable PDUs.

This command syntax determines the power-off period of the power cycling operation for a specific outlet.

```
config:#   outlet <n> cyclingPowerOffPeriod <timing>
```

Variables:

- <n> is the number of the outlet that you want to configure.
- <timing> is the time of the cycling power-off period in seconds, which is an integer between 0 and 3600.

Note: This setting overrides the PDU-defined cycling power-off period on a particular outlet. See **Setting the PDU-Defined Cycling Power-Off Period** *(on page 309).*

Example

The following command sets the power off period of outlet 8 to 3 seconds when the power cycling operation is performed.

```
config:#   outlet 8 cyclingPowerOffPeriod 3
```

Inlet Configuration Commands

An inlet configuration command begins with *inlet*. You can configure an inlet by using the inlet configuration command.

Changing the Inlet Name

This command syntax names an inlet.

```
config:#   inlet <n> name "<name>"
```

Variables:

- <n> is the number of the inlet that you want to configure. For a single-inlet PDU, <n> is always the number 1. The value is an integer between 1 and 50.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Example

The following command assigns the name "AC source" to the inlet 1. If your PX device contains multiple inlets, this command names the 1st inlet.

```
config:#   inlet 1 name "AC source"
```

Circuit Breaker Configuration Commands

A circuit breaker configuration command begins with *ocp.* The command configures an individual circuit breaker.

Changing the Circuit Breaker Name

This command syntax names a circuit breaker.

```
config:#   ocp <n> name "<name>"
```

Variables:

- <n> is the number of the circuit breaker that you want to configure. The value is an integer between 1 and 50.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Example

The command assigns the name "Email servers CB" to the circuit breaker 3.

```
config:#   ocp 3 name "Email servers CB"
```

Environmental Sensor Configuration Commands

An environmental sensor configuration command begins with *externalsensor*. You can configure the name and location parameters of an individual environmental sensor.

Changing the Sensor Name

This command syntax names an environmental sensor.

```
config:#   externalsensor <n> name "<name>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the PX web interface. It is an integer between 1 and 16.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Example

The following command assigns the name "Cabinet humidity" to the environmental sensor with the ID number 4.

```
config:#   externalsensor 4 name "Cabinet humidity"
```

Specifying the Sensor Type

Raritan's contact closure sensor (DPX-CC2-TR) supports the connection of diverse third-party or Raritan's detectors/switches. You must specify the type of connected detector/switch for proper operation. Use this command syntax when you need to specify the sensor type.

```
config:#   externalsensor <n> sensorSubType <type>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the PX web interface. It is an integer between 1 and 16.
- <type> is one of these types: *contact*, *smokeDetection*, *waterDetection* or *vibration*.

Type	Description
contact	The connected detector/switch is for detection of door lock or door closed/open status.
smokeDetection	The connected detector/switch is for detection of the smoke presence.
waterDetection	The connected detector/switch is for detection of the water presence.
vibration	The connected detector/switch is for detection of the vibration.

Example

The following indicates that a smoke detector is being connected to Raritan's contact closure sensor (DPX-CC2-TR) whose ID number shown in the PX web interface is 2.

```
config:#   externalsensor 2 sensorSubType smokeDetection
```

Setting the X Coordinate

This command syntax specifies the X coordinate of an environmental sensor.

```
config:#   externalsensor <n> xlabel "<coordinate>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the PX web interface. It is an integer between 1 and 16.
- <coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.

Example

The following command sets the value "The 2nd cabinet" to the X coordinate of the environmental sensor with the ID number 4.

```
config:#   externalsensor 4 xlabel "The 2nd cabinet"
```

Setting the Y Coordinate

This command syntax specifies the Y coordinate of an environmental sensor.

```
config:#   externalsensor <n> ylabel "<coordinate>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the PX web interface. It is an integer between 1 and 16.
- <coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.

Example

The following command sets the value "The 4th row" to the Y coordinate of the environmental sensor with the ID number 4.

```
config:#   externalsensor 4 ylabel "The 4th row"
```

Setting the Z Coordinate

This command syntax specifies the Z coordinate of an environmental sensor.

config:# externalsensor <n> zlabel "<coordinate>"

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the PX web interface. It is an integer between 1 and 16.
- Depending on the Z coordinate format you set, there are two types of values for the <coordinate> variable:

Type	Description
Free form	<coordinate> is a string comprising up to 24 ASCII printable characters, and it must be enclosed in quotes.
Rack units	<coordinate> is an integer number in rack units.

Note: To specify the Z coordinate using the rack units. See **Setting the Z Coordinate Format for Environmental Sensors** *(on page 312).*

Example

The following command sets the value "The 5th rack" to the Z coordinate of the environmental sensor with the ID number 4 after the Z coordinate's format is set to *freeForm*.

```
config:#   externalsensor 4 zlabel "The 5th rack"
```

Changing the Sensor Description

This command syntax provides a description for a specific environmental sensor.

```
config:#   externalsensor <n> description "<description>"
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the PX web interface. It is an integer between 1 and 16.
- <description> is a string comprising up to 64 ASCII printable characters, and it must be enclosed in quotes.

Example

The following command gives the description "humidity detection" to the environmental sensor with the ID number 4.

```
config:#   externalsensor 4 description "humidity detection"
```

Sensor Threshold Configuration Commands

A sensor configuration command begins with *sensor*. You can use the commands to configure the threshold, hysteresis and assertion timeout values for any sensor associated with the following items:

- Outlets
- Inlets
- Inlet poles (for three-phase PDUs only)
- Circuit breakers
- Environmental sensors

It is permitted to assign a new value to the threshold at any time regardless of whether the threshold is being enabled.

Commands for Outlet Sensors

A sensor configuration command for outlets begins with *sensor outlet*.

Setting the Outlet's Upper Critical Threshold

This command syntax configures the Upper Critical threshold of an outlet.

```
config:#   sensor outlet <n> <sensor type> upperCritical <option>
```

Variables:

- <n> is the number of the outlet that you want to configure.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the upper critical threshold for the specified outlet sensor.
disable	Disables the upper critical threshold for the specified outlet sensor.
A numeric value	Sets a value for the upper critical threshold of the specified outlet sensor and enables this threshold at the same time.

Example

The following command sets the Upper Critical threshold of the outlet 5 RMS current to 18A. It also enables the upper critical threshold if this threshold has not been enabled yet.

```
config:#   sensor outlet 5 current upperCritical 18
```

Setting the Outlet's Upper Warning Threshold

This command syntax configures the Upper Warning threshold of an outlet.

```
config:#   sensor outlet <n> <sensor type> upperWarning <option>
```

Variables:

- <n> is the number of the outlet that you want to configure.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the upper warning threshold for the specified outlet sensor.
disable	Disables the upper warning threshold for the specified outlet sensor.
A numeric value	Sets a value for the upper warning threshold of the specified outlet sensor and enables this threshold at the same time.

Example

The following command enables the Upper Warning threshold of the outlet 5 RMS current.

```
config:#   sensor outlet 5 current upperWarning enable
```

Setting the Outlet's Lower Critical Threshold

This command syntax configures the Lower Critical threshold of an outlet.

```
config:#   sensor outlet <n> <sensor type> lowerCritical <option>
```

Variables:

- <n> is the number of the outlet that you want to configure.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the lower critical threshold for the specified outlet sensor.
disable	Disables the lower critical threshold for the specified outlet sensor.
A numeric value	Sets a value for the lower critical threshold of the specified outlet sensor and enables this threshold at the same time.

Example

The following command sets the Lower Critical threshold for the outlet 5 RMS current to 10A. It also enables the lower critical threshold if this threshold has not been enabled yet.

```
config:#   sensor outlet 5 current lowerCritical 10
```

Setting the Outlet's Lower Warning Threshold

This command syntax configures the Lower Warning threshold of an outlet.

```
config:#   sensor outlet <n> <sensor type> lowerWarning <option>
```

Variables:

- <n> is the number of the outlet that you want to configure.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the lower warning threshold for the specified outlet sensor.
disable	Disables the lower warning threshold for the specified outlet sensor.
A numeric value	Sets a value for the lower warning threshold of the specified outlet sensor and enables this threshold at the same time.

Example

The following command disables the Lower Warning threshold for the outlet 5 RMS current.

```
config:#   sensor outlet 5 current lowerWarning disable
```

Setting the Outlet's Deassertion Hysteresis

This command syntax configures the deassertion hysteresis value of an outlet.

```
config:#   sensor outlet <n> <sensor type> hysteresis <value>
```

Variables:

- <n> is the number of the outlet that you want to configure.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <value> is a numeric value that is assigned to the hysteresis for the specified outlet sensor. See ***What is Deassertion Hysteresis?*** (on page 178) for the function of the deassertion hysteresis.

Example

The following command sets the deassertion hysteresis of the outlet 5 RMS current to 0.2A. That is, the current must drop by at least 0.2A below the upper threshold or rise by at least 0.2A above the lower threshold before any threshold-crossing event is deasserted.

```
config:#   sensor outlet 5 current hysteresis 0.2
```

Setting the Outlet's Assertion Timeout

This command syntax configures the assertion timeout value of an outlet.

```
config:#   sensor outlet <n> <sensor type> assertionTimeout <value>
```

Variables:

- <n> is the number of the outlet that you want to configure.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <value> is a number in samples that is assigned to the assertion timeout for the specified outlet sensor. See ***What is Assertion Timeout?*** (on page 179).

Example

The following command sets the assertion timeout value of the outlet 5 RMS current to 4 samples. That is, at least 4 consecutive samples must cross a specific current threshold before that threshold-crossing event is asserted.

```
config:#   sensor outlet 5 current assertionTimeout 4
```

Commands for Inlet Sensors

A sensor configuration command for inlets begins with *sensor inlet*.

Setting the Inlet's Upper Critical Threshold

This command syntax configures the Upper Critical threshold of an inlet.

```
config:#   sensor inlet <n> <sensor type> upperCritical <option>
```

Variables:

- <n> is the number of the inlet that you want to configure. For a single-inlet PDU, <n> is always the number 1.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the upper critical threshold for the specified inlet sensor.
disable	Disables the upper critical threshold for the specified inlet sensor.
A numeric value	Sets a value for the upper critical threshold of the specified inlet sensor and enables this threshold at the same time.

Example

The following command enables the Upper Critical threshold for the inlet 1 RMS current.

```
config:#   sensor inlet 1 current upperCritical enable
```

Setting the Inlet's Upper Warning Threshold

This command syntax configures the Upper Warning threshold of an inlet.

```
config:#   sensor inlet <n> <sensor type> upperWarning <option>
```

Variables:

- <n> is the number of the inlet that you want to configure. For a single-inlet PDU, <n> is always the number 1.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the upper warning threshold for the specified inlet sensor.
disable	Disables the upper warning threshold for the specified inlet sensor.
A numeric value	Sets a value for the upper warning threshold of the specified inlet sensor and enables this threshold at the same time.

Example

The following command sets the Upper Warning threshold for the inlet 1 RMS current to 12A. It also enables the upper warning threshold if this threshold has not been enabled yet.

```
config:#   sensor inlet 1 current upperWarning 12
```

Setting the Inlet's Lower Critical Threshold

This command syntax configures the Lower Critical threshold of an inlet.

```
config:#   sensor inlet <n> <sensor type> lowerCritical <option>
```

Variables:

- <n> is the number of the inlet that you want to configure. For a single-inlet PDU, <n> is always the number 1.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the lower critical threshold for the specified inlet sensor.
disable	Disables the lower critical threshold for the specified inlet sensor.
A numeric value	Sets a value for the lower critical threshold of the specified inlet sensor and enables this threshold at the same time.

Example

The following command disables the Lower Critical threshold for the inlet 1 RMS current.

```
config:#   sensor inlet 1 current lowerCritical disable
```

Setting the Inlet's Lower Warning Threshold

This command syntax configures the Lower Warning threshold of an inlet.

```
config:#   sensor inlet <n> <sensor type> lowerWarning <option>
```

Variables:

- <n> is the number of the inlet that you want to configure. For a single-inlet PDU, <n> is always the number 1.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the lower warning threshold for the specified inlet sensor.
disable	Disables the lower warning threshold for the specified inlet sensor.
A numeric value	Sets a value for the lower warning threshold of the specified inlet sensor and enables this threshold at the same time.

Example

The following command sets the Lower Warning threshold for the inlet 1 RMS current to 20A. It also enables the lower warning threshold if this threshold has not been enabled yet.

```
config:#   sensor inlet 1 current lowerWarning 20
```

Setting the Inlet's Deassertion Hysteresis

This command syntax configures the deassertion hysteresis value of an inlet.

```
config:#   sensor inlet <n> <sensor type> hysteresis <value>
```

Variables:

- <n> is the number of the inlet that you want to configure. For a single-inlet PDU, <n> is always the number 1.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <value> is a numeric value that is assigned to the hysteresis for the specified inlet sensor. See ***What is Deassertion Hysteresis?*** (on page 178) for the function of the deassertion hysteresis.

Example

The following command sets the deassertion hysteresis for the inlet 1 RMS current to 0.2A. That is, the current must drop by at least 0.2A below the upper threshold or rise by at least 0.2A above the lower threshold before any threshold-crossing event is deasserted.

```
config:#   sensor inlet 1 current hysteresis 0.2
```

Setting the Inlet's Assertion Timeout

This command syntax configures the assertion timeout value of an inlet.

```
config:#   sensor inlet <n> <sensor type> assertionTimeout <value>
```

Variables:

- <n> is the number of the inlet that you want to configure. For a single-inlet PDU, <n> is always the number 1.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <value> is a number in samples that is assigned to the assertion timeout for the specified inlet sensor. See ***What is Assertion Timeout?*** (on page 179).

Example

The following command sets the assertion timeout value of the inlet 1 RMS current to 4 samples. That is, at least 4 consecutive samples must cross a specific current threshold before that threshold-crossing event is asserted.

```
config:#   sensor inlet 1 current assertionTimeout 4
```

Commands for Inlet Pole Sensors

A sensor configuration command for inlet poles begins with *sensor inletpole*. This type of command is available on a three-phase PDU only.

Setting the Upper Critical Threshold for an Inlet Pole

This command syntax configures the Upper Critical threshold of an inlet pole.

```
config:#   sensor inletpole <n> <p> <sensor type> upperCritical <option>
```

Variables:

- <n> is the number of the inlet whose pole sensors you want to configure.
- <p> is the label of the inlet pole that you want to configure.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 - L2
2	**L2**	L2	L2 - L3
3	**L3**	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the upper critical threshold for the specified inlet pole sensor.
disable	Disables the upper critical threshold for the specified inlet pole sensor.
A numeric value	Sets a value for the upper critical threshold of the specified inlet pole sensor and enables this threshold at the same time.

Example

The following command disables the Upper Critical threshold for the pole 3 (L3-L1) voltage of the inlet 1.

```
config:#   sensor inletpole 1 L3 voltage upperCritical disable
```

Setting the Upper Warning Threshold for an Inlet Pole

This command syntax configures the Upper Warning threshold of an inlet pole.

```
config:#   sensor inletpole <n> <p> <sensor type> upperWarning <option>
```

Variables:

- <n> is the number of the inlet whose pole sensors you want to configure.
- <p> is the label of the inlet pole that you want to configure.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 - L2
2	**L2**	L2	L2 - L3
3	**L3**	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the upper warning threshold for the specified inlet pole sensor.
disable	Disables the upper warning threshold for the specified inlet pole sensor.
A numeric value	Sets a value for the upper warning threshold of the specified inlet pole sensor and enables this threshold at the same time.

Example

The following command sets the Upper Warning threshold for the pole 2 (L2-L3) voltage of the inlet 1 to 180V. It also enables the upper warning threshold if this threshold has not been enabled yet.

```
config:#   sensor inletpole 1 L2 voltage upperWarning 180
```

Setting the Lower Critical Threshold for an Inlet Pole

This command syntax configures the Lower Critical threshold of an inlet pole.

```
config:#   sensor inletpole <n> <p> <sensor type> lowerCritical <option>
```

Variables:

- <n> is the number of the inlet whose pole sensors you want to configure.
- <p> is the label of the inlet pole that you want to configure.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 - L2
2	**L2**	L2	L2 - L3
3	**L3**	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor

Sensor type	Description
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the lower critical threshold for the specified inlet pole sensor.
disable	Disables the lower critical threshold for the specified inlet pole sensor.
A numeric value	Sets a value for the lower critical threshold of the specified inlet pole sensor and enables this threshold at the same time.

Example

The following command enables the Lower Critical threshold for the pole 2 (L2-L3) voltage of the inlet 1.

```
config:#   sensor inletpole 1 L2 voltage lowerCritical enable
```

Setting the Lower Warning Threshold for an Inlet Pole

This command syntax configures the Lower Warning threshold of an inlet pole.

```
config:#   sensor inletpole <n> <p> <sensor type> lowerWarning <option>
```

Variables:

- <n> is the number of the inlet whose pole sensors you want to configure.
- <p> is the label of the inlet pole that you want to configure.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 - L2

Pole	Label <p>	Current sensor	Voltage sensor
2	**L2**	L2	L2 - L3
3	**L3**	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the lower warning threshold for the specified inlet pole sensor.
disable	Disables the lower warning threshold for the specified inlet pole sensor.
A numeric value	Sets a value for the lower warning threshold of the specified inlet pole sensor and enables this threshold at the same time.

Example

The following command sets the Lower Warning threshold for the pole 3 (L3-L1) voltage of the inlet 1 to 190V. It also enables the lower warning threshold if this threshold has not been enabled yet.

```
config:#   sensor inletpole 1 L3 voltage lowerWarning 190
```

Setting the Inlet Pole's Deassertion Hysteresis

This command syntax configures the deassertion hysteresis value of an inlet pole.

```
config:#   sensor inletpole <n> <p> <sensor type> hysteresis <value>
```

Variables:

- <n> is the number of the inlet whose pole sensors you want to configure.
- <p> is the label of the inlet pole that you want to configure.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 - L2
2	**L2**	L2	L2 - L3
3	**L3**	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <value> is a numeric value that is assigned to the hysteresis for the specified inlet pole sensor. See ***What is Deassertion Hysteresis?*** (on page 178) for the function of the deassertion hysteresis.

Example

The following command sets the deassertion hysteresis of the pole 2 (L2) current of the inlet 1 to 0.2A. That is, the current must drop by at least 0.2A below the upper threshold or rise by at least 0.2A above the lower threshold before any threshold-crossing event is deasserted.

```
config:#   sensor inletpole 1 L2 current hysteresis 0.2
```

Setting the Inlet Pole's Assertion Timeout

This command syntax configures the assertion timeout value of an inlet pole.

```
config:#   sensor inletpole <n> <p> <sensor type> assertionTimeout <value>
```

Variables:

- <n> is the number of the inlet whose pole sensors you want to configure.
- <p> is the label of the inlet pole that you want to configure.

Pole	Label <p>	Current sensor	Voltage sensor
1	**L1**	L1	L1 - L2
2	**L2**	L2	L2 - L3
3	**L3**	L3	L3 - L1

- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor
voltage	Voltage sensor
activePower	Active power sensor
apparentPower	Apparent power sensor
powerFactor	Power factor sensor
activeEnergy	Active energy sensor
unbalancedCurrent	Unbalanced load sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <value> is a number in samples that is assigned to the assertion timeout for the specified inlet pole sensor. See ***What is Assertion Timeout?*** (on page 179).

Example

The following command sets the assertion timeout value of the pole 2 (L2) current of the inlet 1 to 4 samples. That is, at least 4 consecutive samples must cross a specific current threshold before that threshold-crossing event is asserted.

```
config:#   sensor inletpole 1 L2 current assertionTimeout 4
```

Commands for Circuit Breaker Sensors

A sensor configuration command for circuit breakers begins with *sensor ocp*.

Setting the Upper Critical Threshold for a Circuit Breaker

This command syntax configures the Upper Critical threshold of a circuit breaker.

```
config:#   sensor ocp <n> <sensor type> upperCritical <option>
```

Variables:

- <n> is the number of the circuit breaker that you want to configure.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the upper critical threshold for the specified circuit breaker sensor.
disable	Disables the upper critical threshold for the specified circuit breaker sensor.
A numeric value	Sets a value for the upper critical threshold of the specified circuit breaker sensor and enables this threshold at the same time.

Example

The following command sets the Upper Critical threshold for the 3rd circuit breaker to 16A. It also enables the upper critical threshold if this threshold has not been enabled yet.

```
config:#   sensor ocp 3 current upperCritical 16
```

Setting the Upper Warning Threshold for a Circuit Breaker

This command syntax configures the Upper Warning threshold of a circuit breaker.

```
config:#   sensor ocp <n> <sensor type> upperWarning <option>
```

Variables:

- <n> is the number of the circuit breaker that you want to configure.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the upper warning threshold for the specified circuit breaker sensor.
disable	Disables the upper warning threshold for the specified circuit breaker sensor.
A numeric value	Sets a value for the upper warning threshold of the specified circuit breaker sensor and enables this threshold at the same time.

Example

The following command enables the Upper Warning threshold for the 3rd circuit breaker.

```
config:#   sensor ocp 3 current upperWarning enable
```

Setting the Lower Critical Threshold for a Circuit Breaker

This command syntax configures the Lower Critical threshold of a circuit breaker.

```
config:#   sensor ocp <n> <sensor type> lowerCritical <option>
```

Variables:

- <n> is the number of the circuit breaker that you want to configure.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the lower critical threshold for the specified circuit breaker sensor.
disable	Disables the lower critical threshold for the specified circuit breaker sensor.
A numeric value	Sets a value for the lower critical threshold of the specified circuit breaker sensor and enables this threshold at the same time.

Example

The following command sets the Lower Critical threshold for the 3rd circuit breaker to 5A. It also enables the lower critical threshold if this threshold has not been enabled yet.

```
config:#   sensor ocp 3 current lowerCritical 5
```

Setting the Lower Warning Threshold for a Circuit Breaker

This command syntax configures the Lower Warning threshold of a circuit breaker.

```
config:#   sensor ocp <n> <sensor type> lowerWarning <option>
```

Variables:

- <n> is the number of the circuit breaker that you want to configure.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the lower warning threshold for the specified circuit breaker sensor.
disable	Disables the lower warning threshold for the specified circuit breaker sensor.
A numeric value	Sets a value for the lower warning threshold of the specified circuit breaker sensor and enables this threshold at the same time.

Example

The following command enables the Lower Warning threshold for the 3rd circuit breaker.

```
config:#   sensor ocp 3 current lowerWarning enable
```

Setting the Circuit Breaker's Deassertion Hysteresis

This command syntax configures the deassertion hysteresis value of a circuit breaker.

```
config:#   sensor ocp <n> <sensor type> hysteresis <value>
```

Variables:

- <n> is the number of the circuit breaker that you want to configure.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <value> is a numeric value that is assigned to the hysteresis of the specified circuit breaker sensor. See ***What is Deassertion Hysteresis?*** (on page 178) for the function of the deassertion hysteresis.

Example

The following command sets the deassertion hysteresis of the RMS current of the 3rd circuit breaker to 0.2A. That is, the current must drop by at least 0.2A below the upper threshold or rise by at least 0.2A above the lower threshold before any threshold-crossing event is deasserted.

```
config:#   sensor ocp 3 current hysteresis 0.2
```

Setting the Circuit Breaker's Assertion Timeout

This command syntax configures the assertion timeout value of a circuit breaker.

```
config:#   sensor ocp <n> <sensor type> assertionTimeout <value>
```

Variables:

- <n> is the number of the circuit breaker that you want to configure.
- <sensor type> is one of the following sensor types:

Sensor type	Description
current	Current sensor

Note: If the requested sensor type is not supported, the message "Sensor is not available" is displayed.

- <value> is a number in samples that is assigned to the assertion timeout of the specified circuit breaker sensor. See ***What is Assertion Timeout?*** (on page 179).

Example

The following command sets the assertion timeout value of the RMS current of the 3rd circuit breaker to 4 samples. That is, at least 4 consecutive samples must cross a specific current threshold before that threshold-crossing event is asserted.

```
config:#   sensor ocp 3 current assertionTimeout 4
```

Commands for Environmental Sensors

A sensor threshold configuration command for environmental sensors begins with *sensor externalsensor*.

Setting the Sensor's Upper Critical Threshold

This command syntax configures the Upper Critical threshold of a numeric environmental sensor.

```
config:#   sensor externalsensor <n> <sensor type> upperCritical <option>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the PX web interface. It is an integer between 1 and 16.
- <sensor type> is one of these sensor types: *temperature, humidity, airPressure or air Flow*.

Note: If the specified sensor type does not match the type of the specified environmental sensor, this error message appears: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)," where XXX is the specified sensor type, and <sensortype> is the correct sensor type.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the upper critical threshold for the specified environmental sensor.
disable	Disables the upper critical threshold for the specified environmental sensor.
A numeric value	Sets a value for the upper critical threshold of the specified environmental sensor and enables this threshold at the same time.

Example

The following command sets the Upper Critical threshold of the environmental "temperature" sensor with the ID number 2 to 40 degrees Celsius. It also enables the upper critical threshold if this threshold has not been enabled yet.

```
config:#   sensor externalsensor 2 temperature upperCritical 40
```

Setting the Sensor's Upper Warning Threshold

This command syntax configures the Upper Warning threshold of a numeric environmental sensor.

```
config:#   sensor externalsensor <n> <sensor type> upperWarning <option>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the PX web interface. It is an integer between 1 and 16.
- <sensor type> is one of these sensor types: *temperature, humidity, airPressure or air Flow*.

Note: If the specified sensor type does not match the type of the specified environmental sensor, this error message appears: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)," where XXX is the specified sensor type, and <sensortype> is the correct sensor type.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the upper warning threshold for the specified environmental sensor.

Option	Description
disable	Disables the upper warning threshold for the specified environmental sensor.
A numeric value	Sets a value for the upper warning threshold of the specified environmental sensor and enables this threshold at the same time.

Example

The following command enables the Upper Warning threshold of the environmental "temperature" sensor with the ID number 4.

```
config:#   sensor externalsensor 4 temperature upperWarning enable
```

Setting the Sensor's Lower Critical Threshold

This command syntax configures the Lower Critical threshold of a numeric environmental sensor.

```
config:#   sensor externalsensor <n> <sensor type> lowerCritical <option>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the PX web interface. It is an integer between 1 and 16.
- <sensor type> is one of these sensor types: *temperature, humidity, airPressure or air Flow*.

Note: If the specified sensor type does not match the type of the specified environmental sensor, this error message appears: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)," where XXX is the specified sensor type, and <sensortype> is the correct sensor type.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the lower critical threshold for the specified environmental sensor.
disable	Disables the lower critical threshold for the specified environmental sensor.
A numeric value	Sets a value for the lower critical threshold of the specified environmental sensor and enables this threshold at the same time.

Example

The following command sets the Lower Critical threshold of the environmental "humidity" sensor with the ID number 1 to 15%. It also enables the lower critical threshold if this threshold has not been enabled yet.

```
config:#   sensor externalsensor 1 humidity lowerCritical 15
```

Setting the Sensor's Lower Warning Threshold

This command syntax configures the Lower Warning threshold of a numeric environmental sensor.

```
config:#   sensor externalsensor <n> <sensor type> lowerWarning <option>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the PX web interface. It is an integer between 1 and 16.
- <sensor type> is one of these sensor types: *temperature, humidity, airPressure or air Flow*.

Note: If the specified sensor type does not match the type of the specified environmental sensor, this error message appears: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)," where XXX is the specified sensor type, and <sensortype> is the correct sensor type.

- <option> is one of the options: *enable*, *disable* or a numeric value.

Option	Description
enable	Enables the lower warning threshold for the specified environmental sensor.
disable	Disables the lower warning threshold for the specified environmental sensor.
A numeric value	Sets a value for the lower warning threshold of the specified environmental sensor and enables this threshold at the same time.

Example

The following command disables the Lower Warning threshold of the environmental "humidity" sensor with the ID number 3.

```
config:#   sensor externalsensor 3 humidity lowerWarning disable
```

Setting the Sensor's Deassertion Hysteresis

This command syntax configures the deassertion hysteresis value of a numeric environmental sensor.

```
config:#   sensor externalsensor <n> <sensor type> hysteresis <value>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the PX web interface. It is an integer between 1 and 16.
- <sensor type> is one of these sensor types: *temperature, humidity, airPressure or air Flow*.

  Note: If the specified sensor type does not match the type of the specified environmental sensor, this error message appears: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)," where XXX is the specified sensor type, and <sensortype> is the correct sensor type.
- <value> is a numeric value that is assigned to the hysteresis for the specified environmental sensor. See ***What is Deassertion Hysteresis?*** (on page 178) for the function of the deassertion hysteresis.

Example

The following command sets the deassertion hysteresis of the environmental "temperature" sensor with the ID number 4 to 2 degrees Celsius. That is, the temperature must drop by at least 2 degrees Celsius below the upper threshold or rise by at least 2 degrees Celsius above the lower threshold before any threshold-crossing event is deasserted.

```
config:#   sensor externalsensor 4 temperature hysteresis 2
```

Setting the Sensor's Assertion Timeout

This command syntax configures the assertion timeout value of a numeric environmental sensor.

```
config:#   sensor externalsensor <n> <sensor type> assertionTimeout <value>
```

Variables:

- <n> is the ID number of the environmental sensor that you want to configure. The ID number is assigned and shown in the PX web interface. It is an integer between 1 and 16.
- <sensor type> is one of these sensor types: *temperature, humidity, airPressure or air Flow*.

  Note: If the specified sensor type does not match the type of the specified environmental sensor, this error message appears: "Specified sensor type 'XXX' does not match the sensor's type (<sensortype>)," where XXX is the specified sensor type, and <sensortype> is the correct sensor type.

- <value> is a number in samples that is assigned to the assertion timeout for the specified environmental sensor. See ***What is Assertion Timeout?*** (on page 179).

Example

The following command sets the assertion timeout of the environmental "temperature" sensor with the ID number 3 to 4 samples. That is, at least 4 consecutive samples must cross a specific current threshold before that threshold-crossing event is asserted.

```
config:#   sensor externalsensor 3 temperature assertionTimeout 4
```

User Configuration Commands

Most user configuration commands begin with *user* except for the password change command.

Creating a User Profile

This command syntax creates a new user profile.

```
config:#   user create <name> <option> <roles>
```

After performing the user creation command, the PX prompts you to assign a password to the newly-created user. Then:

1. Type the password and press Enter.
2. Re-type the same password for confirmation and press Enter.

Variables:

- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable CANNOT contain spaces.
- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the newly-created user profile.
disable	Disables the newly-created user profile.

- <roles> is a role or a list of comma-separated roles assigned to the specified user profile.

Example

The following command creates a new user profile and sets two parameters for the new user.

```
config:#   user create May enable admin
```

Results:

- A new user profile "May" is created.
- The new user profile is enabled.
- The **admin** role is assigned to the new user profile.

Modifying a User Profile

A user profile contains various parameters that you can modify.

Tip: You can combine all commands to modify the parameters of a specific user profile at a time. See **Multi-Command Syntax** *(on page 435).*

Changing a User's Password

This command syntax allows you to change an existing user's password if you have the Administrator Privileges.

```
config:#   user modify <name> password
```

After performing the above command, PX prompts you to enter a new password. Then:

1. Type a new password and press Enter.
2. Re-type the new password for confirmation and press Enter.

Variables:

- <name> is the name of the user whose settings you want to change.

Example

The following procedure illustrates how to change the password of the user "May."

1. Verify that you have entered the configuration mode. See ***Entering the Configuration Mode*** (on page 305).
2. Type the following command to change the password for the user profile "May."

   ```
   config:#   user modify May password
   ```
3. Type a new password when prompted, and press Enter.
4. Type the same new password and press Enter.
5. If the password change is completed successfully, the config:# prompt appears.

Modifying a User's Personal Data

You can change a user's personal data, including the user's full name, telephone number, and email address.

- **To change a user's full name, use this command syntax:**

```
config:#   user modify <name> fullName "<full_name>"
```

- **To change a user's telephone number, use this command syntax:**

```
config:#   user modify <name> telephoneNumber "<phone_number>"
```

- **To change a user's email address, use this command syntax:**

```
config:#   user modify <name> eMailAddress <email_address>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <full_name> is a string comprising up to 32 ASCII printable characters. The <full_name> variable must be enclosed in quotes when it contains spaces.
- <phone_number> is the phone number that can reach the specified user. The <phone_number> variable must be enclosed in quotes when it contains spaces.
- <email_address> is the email address of the specified user.

Tip: You can combine all commands to modify the parameters of a specific user profile at a time. See **Multi-Command Syntax** *(on page 435).*

Example

The following command modifies two parameters for the user profile -- May:

```
config:#   user modify May fullName "May Turner" telephoneNumber 123-4567
```

Results:

- May's full name is specified as May Turner.
- May's telephone number is set to 123-4567.

Enabling or Disabling a User Profile

This command syntax enables or disables a user profile. A user can log in to the PX device only after that user's user profile is enabled.

```
config:#   user modify <name> enabled <option>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option> is one of the options: *true* or *false*.

Option	Description
true	Enables the specified user profile.
false	Disables the specified user profile.

Example

The following command enables the user profile -- May.

```
config:#   user modify May enabled true
```

Forcing a Password Change

This command syntax determines whether the password change is forced when a user logs in to the specified user profile next time.

```
config:#   user modify <name> forcePasswordChangeOnNextLogin <option>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option> is one of the options: *true* or *false*.

Option	Description
true	A password change is forced on the user's next login.
false	No password change is forced on the user's next login.

Example

The following command enforces a password change on May's next login.

```
config:#   user modify May forcePasswordChangeOnNextLogin true
```

Modifying the SNMPv3 Settings

There are different commands to modify the SNMPv3 parameters of a specific user profile. You can combine all of the following commands to modify the SNMPv3 parameters at a time. See ***Multi-Command Syntax*** (on page 435).

To enable or disable the SNMP v3 access to PX for the specified user:

```
config:#   user modify <name> snmpV3Access <option1>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option1> is one of the options: *enable* or *disable*.

Option	Description
enable	Enables the SNMP v3 access permission for the specified user.
disable	Disables the SNMP v3 access permission for the specified user.

To determine the security level:

```
config:#   user modify <name> securityLevel <option2>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option2> is one of the options: *noAuthNoPriv*, *authNoPriv* or *authPriv*.

Option	Description
noAuthNoPriv	No authentication and no privacy.
authNoPriv	Authentication and no privacy.
authPriv	Authentication and privacy.

To determine whether the authentication passphrase is identical to the password:

```
config:#    user modify <name> userPasswordAsAuthenticationPassphrase <option3>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option3> is one of the options: *true* or *false*.

Option	Description
true	Authentication passphrase is identical to the password.
false	Authentication passphrase is different from the password.

To determine the authentication passphrase:

```
config:#    user modify <name> authenticationPassPhrase <authentication_passphrase>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <authentication_passphrase> is a string used as an authentication passphrase, comprising up to 32 ASCII printable characters.

To determine whether the privacy passphrase is identical to the authentication passphrase:

```
config:#    user modify <name> useAuthenticationPassPhraseAsPrivacyPassPhrase <option4>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option4> is one of the options: *true* or *false*.

Option	Description
true	Privacy passphrase is identical to the authentication passphrase.

Option	Description
false	Privacy passphrase is different from the authentication passphrase.

To determine the privacy passphrase:

```
config:#   user modify <name> privacyPassPhrase <privacy_passphrase>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <privacy_passphrase> is a string used as a privacy passphrase, comprising up to 32 ASCII printable characters.

To determine the authentication protocol:

```
config:#   user modify <name> authenticationProtocol <option5>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option5> is one of the options: *MD5* or *SHA-1*.

Option	Description
MD5	MD5 authentication protocol is applied.
SHA-1	SHA-1 authentication protocol is applied.

To determine the privacy protocol:

```
config:#   user modify <name> privacyProtocol <option6>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option6> is one of the options: *DES* or *AES-128*.

Option	Description
DES	DES privacy protocol is applied.

Option	Description
AES-128	AES-128 privacy protocol is applied.

Example

The following command sets three SNMPv3 parameters of the user "May."

```
config:#   user modify May snmpV3Access enable securityLevel authNoPriv
           userPasswordAsAuthenticationPassPhrase true
```

Results:

- The user's SNMPv3 access permission is enabled.
- The SNMPv3 security level is authentication only, no privacy.
- The authentication passphrase is identical to the user's password.

Changing the Role(s)

This command syntax changes the role(s) of a specific user.

```
config:#   user modify <name> roles <roles>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <roles> is a role or a list of comma-separated roles assigned to the specified user profile.

Example

The following command assigns two roles to the user "May."

```
config:#   user modify May roles admin,tester
```

Results:

- The user May has the union of all privileges of "admin" and "tester."

Changing the Measurement Units

You can change the measurement units displayed for temperatures, length, and pressure for a specific user profile. Different measurement unit commands can be combined so that you can set all measurement units at a time. To combine all commands, see ***Multi-Command Syntax*** (on page 435).

Note: The measurement unit change only applies to the web interface and command line interface.

Tip: To set the default measurement units applied to the PX user interfaces for all users via CLI, see **Setting Default Measurement Units** *(on page 416).*

To set the preferred temperature unit:

```
config:#   user modify <name> preferredTemperatureUnit <option1>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option1> is one of the options: *C* or *F*.

Option	Description
C	This option displays the temperature in Celsius.
F	This option displays the temperature in Fahrenheit.

To set the preferred length unit:

```
config:#   user modify <name> preferredLengthUnit <option2>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option2> is one of the options: *meter* or *feet*.

Option	Description
meter	This option displays the length or height in meters.
feet	This option displays the length or height in feet.

To set the preferred pressure unit:

```
config:#   user modify <name> preferredPressureUnit <option3>
```

Variables:

- <name> is the name of the user whose settings you want to change.
- <option3> is one of the options: *pascal* or *psi*.

Option	Description
pascal	This option displays the pressure value in Pascals (Pa).
psi	This option displays the pressure value in psi.

Example

The following command sets all measurement unit preferences for the user "May."

```
config:#   user modify May preferredTemperatureUnit F preferredLengthUnit feet
preferredPressureUnit psi
```

Results:

- The preferred temperature unit is set to Fahrenheit.
- The preferred length unit is set to feet.
- The preferred pressure unit is set to psi.

Deleting a User Profile

This command syntax deletes an existing user profile.

```
config:#   user delete <name>
```

Example

The following command deletes the user profile "May."

```
config:#   user delete May
```

Changing Your Own Password

Every user can change their own password via this command syntax if they have the Change Own Password privilege. Note that this command does not begin with *user*.

```
config:#   password
```

After performing this command, the PX prompts you to enter both current and new passwords respectively.

Important: After the password is changed successfully, the new password is effective immediately no matter you type the command "apply" or not to save the changes.

Example

This procedure changes your own password:

1. Verify that you have entered the configuration mode. See ***Entering the Configuration Mode*** (on page 305).
2. Type the following command and press Enter.

   ```
   config:#   password
   ```

3. Type the existing password and press Enter when the following prompt appears.

   ```
   Current password:
   ```

4. Type the new password and press Enter when the following prompt appears.

   ```
   Enter new password:
   ```

5. Re-type the new password for confirmation and press Enter when the following prompt appears.

   ```
   Re-type new password:
   ```

Setting Default Measurement Units

Default measurement units, including temperature, length, and pressure units, apply to the PX user interfaces across all users except for those who have changed their own preferred measurement units or those whose preferred measurement units are set differently by the administrator. Different measurement unit commands can be combined so that you can set all default measurement units at a time. To combine all commands, see ***Multi-Command Syntax*** (on page 435).

Note: The measurement unit change only applies to the web interface and command line interface.

Tip: To change the preferred measurement units displayed in the PX user interfaces for a specific user via CLI, see **Changing the Measurement Units** *(on page 413)*.

To set the default temperature unit:

```
config:#   user defaultpreferences preferredTemperatureUnit <option1>
```

Variables:

- <option1> is one of the options: *C* or *F*.

Option	Description
C	This option displays the temperature in Celsius.
F	This option displays the temperature in Fahrenheit.

To set the default length unit:

```
config:#   user defaultpreferences preferredLengthUnit <option2>
```

Variables:

- <option2> is one of the options: *meter* or *feet*.

Option	Description
meter	This option displays the length or height in meters.
feet	This option displays the length or height in feet.

To set the default pressure unit:

```
config:#    user defaultpreferences preferredPressureUnit <option3>
```

Variables:

- <option3> is one of the options: *pascal* or *psi*.

Option	Description
pascal	This option displays the pressure value in Pascals (Pa).
psi	This option displays the pressure value in psi.

Example

The following command sets all default measurement units at a time.

```
config:#    user defaultpreferences preferredTemperatureUnit F preferredLengthUnit feet
            preferredPressureUnit psi
```

Results:

- The default temperature unit is set to Fahrenheit.
- The default length unit is set to feet.
- The default pressure unit is set to psi.

Role Configuration Commands

A role configuration command begins with *role*.

Creating a Role

This command syntax creates a new role, with a list of semicolon-separated privileges assigned to the role.

```
config:#    role create <name> <privilege1>;<privilege2>;<privilege3>...
```

If a specific privilege contains any arguments, that privilege should be followed by a colon and the argument(s).

```
config:#    role create <name> <privilege1>:<argument1>,<argument2>...;
            <privilege2>:<argument1>,<argument2>...;
            <privilege3>:<argument1>,<argument2>...;
            ...
```

Variables:

- <name> is a string comprising up to 32 ASCII printable characters.
- <privilege1>, <privilege2>, <privilege3> and the like are names of the privileges assigned to the role. Separate each privilege with a semi-colon. See ***All Privileges*** (on page 418).
- <argument1>, <argument2> and the like are arguments set for a particular privilege. Separate a privilege and its argument(s) with a colon, and separate arguments with a comma if there are more than one argument for a privilege.

All Privileges

This table lists all privileges. Note that available privileges vary according to the model you purchased. For example, a PDU without the outlet switching function does not have the privilege "switchOutlet."

Privilege	Description
adminPrivilege	Administrator Privileges
changeAssetStripConfiguration	Change Asset Strip Configuration
changeAuthSettings	Change Authentication Settings
changeDataTimeSettings	Change Date/Time Settings
changeEventSetup	Change Event Settings
changeExternalSensorsConfiguration	Change External Sensors Configuration
changeLhxConfiguration	Change LHX Configuration
changeNetworkSettings	Change Network Settings
changePassword	Change Own Password
changePduConfiguration	Change Pdu, Inlet, Outlet & Overcurrent Protector Configuration
changeStsConfiguration	Change STS Configuration
changeSecuritySettings	Change Security Settings
changeSnmpSettings	Change SNMP Settings

Privilege	Description
changeUserSettings	Change Local User Management
changeWebcamSettings	Change Webcam Configuration
clearLog	Clear Local Event Log
firmwareUpdate	Firmware Update
performReset	Reset (Warm Start)
switchOutlet*	Switch Outlet
viewEventSetup	View Event Settings
viewLog	View Local Event Log
viewSecuritySettings	View Security Settings
viewSnmpSettings	View SNMP Settings
viewUserSettings	View Local User Management
viewWebcamSettings	View Webcam Snapshots and Configuration

* The "switchOutlet" privilege requires an argument that is separated with a colon. The argument could be:

- All outlets, that is,
  `switchOutlet:all`
- An outlet number. For example:
  `switchOutlet:1`
  `switchOutlet:2`
  `switchOutlet:3`
- A list of comma-separated outlets. For example:
  `switchOutlet:1,3,5,7,8,9`

Example

The following command creates a new role and assigns privileges to the role.

```
config:#   role create tester firmwareUpdate;viewEventSetup
```

Results:

- A new role "tester" is created.
- Two privileges are assigned to the role: firmwareUpdate (Firmware Update) and viewEventSetup (View Event Settings).

Modifying a Role

You can modify diverse parameters of an existing role, including its privileges.

To modify a role's description:

```
config:#   role modify <name> description "<description>"
```

Variables:

- <name> is a string comprising up to 32 ASCII printable characters.
- <description> is a description comprising alphanumeric characters. The <description> variable must be enclosed in quotes when it contains spaces.

To add more privileges to a specific role:

```
config:#   role modify <name> addPrivileges
           <privilege1>;<privilege2>;<privilege3>...
```

If a specific privilege contains any arguments, add a colon and the argument(s) after that privilege.

```
config:#   role modify <name> addPrivileges
           <privilege1>:<argument1>,<argument2>...;
           <privilege2>:<argument1>,<argument2>...;
           <privilege3>:<argument1>,<argument2>...;
           ...
```

Variables:

- <name> is a string comprising up to 32 ASCII printable characters.
- <privilege1>, <privilege2>, <privilege3> and the like are names of the privileges assigned to the role. Separate each privilege with a semi-colon. See ***All Privileges*** (on page 418).
- <argument1>, <argument2> and the like are arguments set for a particular privilege. Separate a privilege and its argument(s) with a colon, and separate arguments with a comma if there are more than one argument for a privilege.

To remove specific privileges from a role:

```
config:#   role modify <name> removePrivileges
           <privilege1>;<privilege2>;<privilege3>...
```

If a specific privilege contains any arguments, add a colon and the argument(s) after that privilege.

```
config:#   role modify <name> removePrivileges
           <privilege1>:<argument1>,<argument2>...;
           <privilege2>:<argument1>,<argument2>...;
           <privilege3>:<argument1>,<argument2>...;
           ...
```

Note: When removing privileges from a role, make sure the specified privileges and arguments (if any) exactly match those assigned to the role. Otherwise, the command fails to remove specified privileges that are not available.

Variables:

- <name> is a string comprising up to 32 ASCII printable characters.
- <privilege1>, <privilege2>, <privilege3> and the like are names of the privileges assigned to the role. Separate each privilege with a semi-colon. See ***All Privileges*** (on page 418).
- <argument1>, <argument2> and the like are arguments set for a particular privilege. Separate a privilege and its argument(s) with a colon, and separate arguments with a comma if there are more than one argument for a privilege.

Example

The following command modifies the privileges of the role "tester."

```
config:#   role modify tester addPrivileges changeAuthSettings removePrivileges
           firmwareUpgrade
```

Results:

- The "changeAuthSettings" (Change Authentication Settings) privilege is added to the role.
- The "firmwareUpgrade" (Firmware Upgrade) privilege is removed from the role.

Deleting a Role

This command syntax deletes an existing role.

```
config:#   role delete <name>
```

Example

The following command deletes an existing role.

```
config:#   role delete tester
```

EnergyWise Configuration Commands

An EnergyWise configuration command begins with *energywise*.

Enabling or Disabling EnergyWise

This command syntax determines whether the Cisco® EnergyWise endpoint implemented on the PX device is enabled.

```
config:#   energywise enabled <option>
```

Variables:

- <option> is one of the options: *true* or *false*.

Option	Description
true	The Cisco EnergyWise feature is enabled.
false	The Cisco EnergyWise feature is disabled.

Example

The following command enables the Cisco® EnergyWise feature.

```
config:#   energywise enabled true
```

Specifying the EnergyWise Domain

This command syntax specifies to which Cisco® EnergyWise domain the PX device belongs.

```
config:#   energywise domain <name>
```

Variables:

- <name> is a string comprising up to 127 ASCII printable characters. Spaces and asterisks are NOT acceptable.

Example

The following command configures the PX device to belong to the Cisco® EnergyWise domain named "helloDomain."

```
config:#   energywise domain helloDomain
```

Specifying the EnergyWise Secret

This command syntax specifies the password (secret) to enter the Cisco® EnergyWise domain.

```
config:#   energywise secret <password>
```

Variables:

- <password> is a string comprising up to 127 ASCII printable characters. Spaces and asterisks are NOT acceptable.

Example

The following command specifies "password5233" as the Cisco® EnergyWise domain secret (password).

```
config:#   energywise secret password5233
```

Changing the UDP Port

This command syntax specifies the UDP port for communications in the Cisco® EnergyWise domain.

```
config:#   energywise port <port>
```

Variables:

- <port> is the UDP port number ranging between 1 and 65535.

Example

The following command specifies 10288 as the UDP port for Cisco® EnergyWise.

```
config:#   energywise port 10288
```

Setting the Polling Interval

This command syntax determines the polling interval at which the Cisco® EnergyWise domain queries the PX device.

```
config:#   energywise polling <timing>
```

Variables:

- <timing> is an integer number in seconds. It ranges between 30 and 600 seconds.

Example

The following command determines the polling interval to query the PX device is 300 seconds.

```
config:#   energywise polling 300
```

Asset Management Commands

You can use the CLI commands to change the settings of the connected asset sensor (if any) or the settings of LEDs on the asset sensor.

Asset Sensor Management

An asset sensor management configuration command begins with `assetStrip`.

Naming an Asset Sensor

This command syntax names or changes the name of an asset sensor connected to the PX device.

```
config:#   assetStrip <n> name "<name>"
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the PX device with only one FEATURE port, the number is always 1.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Example

This command syntax names or changes the name of an asset sensor connected to the PX device.

```
config:#   assetStrip 1 name "Red Rack"
```

Specifying the Number of Rack Units

This command syntax specifies the total number of rack units on an asset sensor connected to the PX device.

```
config:#   assetStrip <n> numberOfRackUnits <number>
```

Note: For the Raritan asset sensor, a rack unit refers to a tag port.

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the PX device with only one FEATURE port, the number is always 1.
- <number> is the total number of rack units available on the connected asset sensor. This value ranges from 8 to 64.

Example

The following command specifies the total number of rack units on the asset sensor #1 to 48 rack units.

```
config:#   assetStrip 1 numberOfRackUnits 48
```

Specifying the Rack Unit Numbering Mode

This command syntax specifies the numbering mode of rack units on the asset sensors connected to the PX device. The numbering mode changes the rack unit numbers.

```
config:#   assetStrip <n> rackUnitNumberingMode <mode>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the PX device with only one FEATURE port, the number is always 1.
- <mode> is one of the numbering modes: *topDown* or *bottomUp*.

Mode	Description
topDown	The rack units are numbered in the ascending order from the highest to the lowest rack unit.
bottomUp	The rack units are numbered in the descending order from the highest to the lowest rack unit.

Example

The following command causes the rack units of the asset sensor #1 to be numbered in an ascending order from the one closest to the asset sensor's RJ-45 connector to the farthest one. That is, the rack unit that is most close to the RJ-45 connector is numbered 1.

```
config:#   assetStrip 1 rackUnitNumberingMode topDown
```

Specifying the Rack Unit Numbering Offset

This command syntax specifies the starting number of rack units on the asset sensors connected to the PX device.

```
config:#   assetStrip <n> rackUnitNumberingOffset <number>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the PX device with only one FEATURE port, the number is always 1.
- <number> is a starting number for numbering rack units on the connected asset sensor. This value is an integer number.

Example

The following command specifies the starting number of rack units of the asset sensor #1 to be 5. That is, the rack units are numbered 5, 6, 7 and so on from the first to the final rack unit on the asset sensor #1.

```
config:#   assetStrip 1 rackUnitNumberingOffset 5
```

Specifying the Asset Sensor Orientation

This command syntax specifies the orientation of the asset sensors connected to the PX device. Usually you do not need to perform this command unless your asset sensors do NOT come with the tilt sensor, causing the PX unable to detect the asset sensors' orientation.

```
config:#   assetStrip <n> assetStripOrientation <orientation>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the PX device with only one FEATURE port, the number is always 1.
- <orientation> is one of the options: *topConnector* or *bottomConnector*.

Orientation	Description
topConnector	This option indicates that the asset sensor is mounted with the RJ-45 connector located on the top.
bottomConnector	This option indicates that the asset sensor is mounted with the RJ-45 connector located at the bottom.

Example

The following command specifies the orientation of the RJ-45 connector on the asset sensor #1 to be on the top.

```
config:#   assetStrip 1 assetStripOrientation topConnector
```

Setting LED Colors for Connected Tags

This command syntax sets the LED color for all rack units on the asset sensor #1 to indicate the presence of a connected asset tag.

```
config:#   assetStrip <n> LEDColorForConnectedTags <color>
```

Variables:

- <color> is the hexadecimal RGB value of a color in HTML format. The <color> variable ranges from #000000 to #FFFFFF.

Example

The following command sets the LED color for all rack units on the asset sensor #1 to RED (that is, FF0000) to indicate the presence of a connected asset tag.

```
config:#   assetStrip 1 LEDColorForConnectedTags #FF0000
```

Setting LED Colors for Disconnected Tags

This command syntax sets the LED color for all rack units on the connected asset sensor(s) to indicate the absence of a connected asset tag.

```
config:#   assetStrip <n> LEDColorForDisconnectedTags <color>
```

Variables:

- <color> is the hexadecimal RGB value of a color in HTML format. The <color> variable ranges from #000000 to #FFFFFF.

Example

This command syntax sets the LED color for all rack units on the asset sensor #1 to BLACK (that is, 000000) to indicate the absence of a connected asset tag.

```
config:#   assetStrip 1 LEDColorForDisconnectedTags #000000
```

Note: Black color causes the LEDs to stay off.

Rack Unit Configuration

For the Raritan asset sensor, a rack unit refers to a tag port. A rack unit configuration command begins with `rackUnit`.

Naming a Rack Unit

This command syntax assigns or changes the name of the specified rack unit on the specified asset sensor.

```
config:#   rackUnit <n> <rack_unit> name "<name>"
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the PX device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit. The index number of each rack unit is available on the Asset Strip page of the web interface.
- <name> is a string comprising up to 32 ASCII printable characters. The <name> variable must be enclosed in quotes when it contains spaces.

Example

The following command assigns the name "Linux server" to the rack unit whose index number is 25 on the asset sensor#1.

```
config:#   rackUnit 1 25 name "Linux server"
```

Setting the LED Operation Mode

This command syntax determines whether a specific rack unit on the specified asset sensor follows the global LED color settings.

```
config:#   rackUnit <n> <rack_unit> LEDOperationMode <mode>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the PX device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit. The index number of each rack unit is available on the Asset Strip page of the web interface.
- <mode> is one of the LED modes: *automatic* or *manual*.

Mode	Description
automatic	This option makes the LED of the specified rack unit follow the global LED color settings. See ***Setting LED Colors for Connected Tags*** (on page 429) and ***Setting LED Colors for Disconnected Tags*** (on page 429). This is the default.
manual	This option enables selection of a different LED color and LED mode for the specified rack unit. When this option is selected, see ***Setting an LED Color for a Rack Unit*** (on page 432) and ***Setting an LED Mode for a Rack Unit*** (on page 433) to set different LED settings.

Example

The following command allows the rack unit whose index number is 25 on the asset sensor#1 to have a different LED color and mode.

```
config:#   rackUnit 1 25 LEDOperationMode manual
```

Setting an LED Color for a Rack Unit

This command syntax sets the LED color for a specific rack unit on the specified asset sensor. You need to set a rack unit's LED color only when the LED operation mode of this rack unit has been set to "manual."

```
config:#   rackUnit <n> <rack_unit> LEDColor <color>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the PX device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit. The index number of each rack unit is available on the Asset Strip page of the web interface.
- <color> is the hexadecimal RGB value of a color in HTML format. The <color> variable ranges from #000000 to #FFFFFF.

Note: A rack unit's LED color setting overrides the global LED color setting on it. See **Setting LED Colors for Connected Tags** *(on page 429) and* **Setting LED Colors for Disconnected Tags** *(on page 429).*

Example

The following command sets the LED color of the rack unit whose index number is 25 on the asset sensor#1 to PINK (that is, FF00FF).

```
config:#   rackUnit 1 25 LEDColor #FF00FF
```

Setting an LED Mode for a Rack Unit

This command syntax sets the LED mode for a specific rack unit on the specified asset sensor. You need to set a rack unit's LED mode only when the LED operation mode of this rack unit has been set to "manual."

```
config:#   rackUnit <n> <rack_unit> LEDMode <mode>
```

Variables:

- <n> is the number of the FEATURE port where the selected asset sensor is physically connected. For the PX device with only one FEATURE port, the number is always 1.
- <rack_unit> is the index number of the desired rack unit. The index number of each rack unit is available on the Asset Strip page of the web interface.
- <mode> is one of the LED modes: *on*, *off*, *blinkSlow* or *blinkFast*.

Mode	Description
on	This mode has the LED stay lit permanently.
off	This mode has the LED stay off permanently.
blinkSlow	This mode has the LED blink slowly.
blinkFast	This mode has the LED blink quickly.

Example

The following command causes the LED of the rack unit whose index number is 25 on the asset sensor#1 to blink quickly.

```
config:#   rackUnit 1 25 LEDMode blinkFast
```

Serial Port Configuration Commands

A serial port configuration command begins with *serial*.

Setting the Serial Port Baud Rate

The following command syntax sets the baud rate (bps) of the serial port labeled CONSOLE / MODEM on the PX device. Change the baud rate before connecting it to any Raritan device, such as Raritan's P2CIM-SER, through the serial port, or there are communications errors. If you change the baud rate dynamically after the connection has been made, you must reset the PX or power cycle the other Raritan device for proper communications.

```
config:#   serial baudRate <baud_rate>
```

Variables:

- <baud_rate> is one of the baud rate options: *1200*, *2400*, *4800*, *9600*, *19200*, *38400*, *57600*, *115200*.

Note: The serial port setting is especially useful when the PX works in conjunction with Raritan's Dominion LX KVM switch. The Dominion LX only supports 19200 bps for communications over the serial interface.

Example

The following command sets the baud rate of the PX device's serial port to 9600 bps.

```
config:#   serial baudRate 9600
```

Setting the History Buffer Length

This command syntax sets the history buffer length, which determines the amount of history commands that can be retained in the buffer. The default length is 25.

```
config:#   history length <n>
```

Variables:

- <n> is an integer number between 1 and 250.
- If you leave the <n> variable blank when using the command, the history buffer is set to 25 by default.

Multi-Command Syntax

To shorten the configuration time, you can combine various configuration commands in one command and perform all of them at a time.

A multi-command syntax looks like this:

```
<setting 1> <value 1> <setting 2> <value 2> <setting 3>
<value 3> ...
```

Example 1 - Combination of IP, Subnet Mask and Gateway Parameters

The following multi-command syntax configures IPv4 address, subnet mask and gateway for the network connectivity simultaneously.

```
config:#   network ipv4 ipAddress 192.168.84.225 subnetMask
           255.255.255.0 gateway 192.168.84.0
```

Results:

- The IP address is set to 192.168.84.225.
- The subnet mask is set to 255.255.255.0.
- The gateway is set to 192.168.84.0.

Example 2 - Combination of Upper Critical and Upper Warning Settings

The following multi-command syntax simultaneously configures Upper Critical and Upper Warning thresholds for the RMS current of the 3rd circuit breaker.

```
config:#   sensor ocp 3 current upperCritical disable upperWarning 20
```

Results:

- The Upper Critical threshold of the 3rd circuit breaker's RMS current is disabled.
- The Upper Warning threshold of the 3rd circuit breaker's RMS current is set to 20A and enabled at the same time.

Example 3 - Combination of SSID and PSK Parameters

This multi-command syntax configures both of SSID and PSK parameters simultaneously for the wireless feature.

```
config:#   network wireless SSID myssid PSK encryp_key
```

Results:

- The SSID value is set to myssid.
- The PSK value is set to encryp_key.

Example 4 - Combination of Upper Critical, Upper Warning and Lower Warning Settings

The following multi-command syntax configures Upper Critical, Upper Warning and Lower Warning thresholds for the outlet 5 RMS current simultaneously.

```
config:#   sensor outlet 5 current upperCritical disable upperWarning enable
           lowerWarning 1.0
```

Results:

- The Upper Critical threshold of outlet 5 RMS current is disabled.
- The Upper Warning threshold of outlet 5 RMS current is enabled.
- The Lower Warning threshold of outlet 5 RMS current is set to 1.0A and enabled at the same time.

Quitting the Configuration Mode

Both of "apply" and "cancel" commands let you quit the configuration mode. The difference is that "apply" saves all changes you made in the configuration mode while "cancel" aborts all changes.

To quit the configuration mode, use either command:

```
config:#    apply
```

-- OR --

```
config:#    cancel
```

The # prompt appears after pressing Enter, indicating that you have entered the administrator mode.

Load Shedding Configuration Commands

This section only applies to outlet-switching capable PDUs.

A load shedding configuration command begins with *loadshedding*.

Unlike other CLI configuration commands, the load shedding configuration command is performed in the *administrator mode* rather than the configuration mode. See ***Different CLI Modes and Prompts*** (on page 276).

Enabling or Disabling Load Shedding

This section only applies to outlet-switching capable PDUs.

This command syntax determines whether the load shedding feature is enabled.

```
#           loadshedding <option>
```

After performing the above command, PX prompts you to confirm the operation. Press y to confirm or n to abort the operation.

To skip the confirmation step, you can add the "/y" parameter to the end of the command so that the operation is executed immediately.

```
#           loadshedding <option> /y
```

Variables:

- <option> is one of the options: *enable* or *disable*.

Option	Description
enable	The load shedding feature is enabled.
disable	The load shedding feature is disabled.

Example

The following command enables the load shedding feature.

```
config:#    loadshedding enable
```

Power Control Operations

This section only applies to outlet-switching capable PDUs.

Outlets on the PX device can be turned on or off or power cycled through the CLI.

You must perform this operation in the *administrator mode*. See ***Different CLI Modes and Prompts*** (on page 276).

Turning On the Outlet(s)

This section only applies to outlet-switching capable PDUs.

This command syntax turns on one or multiple outlets.

```
#       power outlets <numbers> on
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

```
#       power outlets <numbers> on /y
```

Variables:

- <numbers> is one of the options: *all*, an outlet number, a list or a range of outlets.

Option	Description
all	Switches ON all outlets.
A specific outlet number	Switches ON the specified outlet.
A comma-separated list of outlets	Switches ON multiple, inconsecutive or consecutive outlets. For example, to specify 7 outlets -- 2, 4, 9, 11, 12, 13 and 15, type `outlets 2,4,9,11-13,15`.
A range of outlets with an en dash in between	Switches ON multiple, consecutive outlets. For example, to specify 6 consecutive outlets -- 3, 4, 5, 6, 7, 8, type `outlets 3-8`.

If you entered the command without "/y", a message appears, prompting you to confirm the operation. Then:

- Type y to confirm the operation, OR
- Type n to abort the operation

Example

The following command turns on all outlets.

```
#     power outlets all on
```

Turning Off the Outlet(s)

This section only applies to outlet-switching capable PDUs.

This command syntax turns off one or multiple outlets.

```
#       power outlets <numbers> off
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

```
#       power outlets <numbers> off /y
```

Variables:

- <numbers> is one of the options: *all*, an outlet number, a list or a range of outlets.

Option	Description
all	Switches OFF all outlets.
A specific outlet number	Switches OFF the specified outlet.
A comma-separated list of outlets	Switches OFF multiple, inconsecutive or consecutive outlets. For example, to specify 7 outlets -- 2, 4, 9, 11, 12, 13 and 15, type `outlets 2,4,9,11-13,15`.

Option	Description
A range of outlets with an en dash in between	Switches OFF multiple, consecutive outlets. For example, to specify 6 consecutive outlets -- 3, 4, 5, 6, 7, 8, type `outlets 3-8`.

If you entered the command without "/y", a message appears, prompting you to confirm the operation. Then:

- Type y to confirm the operation, OR
- Type n to abort the operation

Example

The following command turns off the outlet 6.

```
#     power outlets 6 off
```

Power Cycling the Outlet(s)

This section only applies to outlet-switching capable PDUs.

This command syntax power cycles one or multiple outlets.

```
#       power outlets <numbers> cycle
```

To quicken the operation, you can add the parameter "/y" to the end of the command, which confirms the operation.

```
#       power outlets <numbers> cycle /y
```

Variables:

- <numbers> is one of the options: *all*, an outlet number, a list or a range of outlets.

Option	Description
all	Power cycles all outlets.
A specific outlet number	Power cycles the specified outlet.

Option	Description
A comma-separated list of outlets	Power cycles multiple, inconsecutive or consecutive outlets. For example, to specify 7 outlets -- 2, 4, 9, 11, 12, 13 and 15, type `outlets 2,4,9,11-13,15`.
A range of outlets with an en dash in between	Power cycles multiple, consecutive outlets. For example, to specify 6 consecutive outlets -- 3, 4, 5, 6, 7, 8, type `outlets 3-8`.

If you entered the command without "/y", a message appears, prompting you to confirm the operation. Then:

- Type y to confirm the operation, OR
- Type n to abort the operation

Example

The following command power cycles these outlets: 2, 6, 7, 8, 10, 13, 14, 15 and 16.

```
#     power outlets 2,6-8,10,13-16 cycle
```

Unblocking a User

If any user is blocked from accessing the PX, you can unblock them at the local console.

To unblock a user:

1. Log in to the CLI interface using any terminal program via a local connection. See ***With HyperTerminal*** (on page 274).
2. When the Username prompt appears, type `unblock` and press Enter.

```
Username: unblock
```

3. When the "Username to unblock" prompt appears, type the login name of the user to be unblocked and press Enter.

```
Username to unblock:
```

4. A message appears, indicating that the specified user was unblocked successfully.

Resetting the PX

You can reset the PX device to factory defaults or simply restart it using the CLI commands.

Restarting the PDU

This command restarts the PX device. It is not a factory default reset.

To restart the PX device:

1. Ensure you have entered the administrator mode and the # prompt is displayed.
2. Type either of the following commands to restart the PX device.

   ```
   #     reset unit
   ```

   -- OR --

   ```
   #     reset unit /y
   ```

3. If you entered the command without "/y" in Step 2, a message appears prompting you to confirm the operation. Type y to confirm the reset.
4. Wait until the Username prompt appears, indicating the reset is complete.

Resetting to Factory Defaults

This command restores all settings of the PX device to factory defaults.

To reset PX settings, use either command:

```
#     reset factorydefaults
```

-- OR --

```
#     reset factorydefaults /y
```

See ***Using the CLI Command*** (on page 468) for more information.

Network Troubleshooting

The PX provides 4 diagnostic commands for troubleshooting network problems: *nslookup*, *netstat*, *ping*, and *traceroute*. The diagnostic commands function as corresponding Linux commands and can get corresponding Linux outputs.

Entering the Diagnostic Mode

Diagnostic commands function in the diagnostic mode only.

To enter the diagnostic mode:

1. Ensure you have entered the administrator mode and the # prompt is displayed.
2. Type `diag` and press Enter. The diag> prompt appears, indicating that you have entered the diagnostic mode.
3. Now you can type any diagnostic commands for troubleshooting.

Diagnostic Commands

The diagnostic command syntax varies from command to command.

Querying the DNS Servers

This command syntax queries Internet domain name server (DNS) information of a network host.

```
diag>       nslookup <host>
```

Variables:

- <host> is the name or IP address of the host whose DNS information you want to query.

Example

The following command checks the DNS information regarding the host 192.168.84.222.

```
diag>       nslookup 192.168.84.222
```

Showing the Network Connections

This command syntax displays network connections and/or status of ports.

```
diag>       netstat <option>
```

Variables:

- <option> is one of the options: *ports* or *connections*.

Option	Description
ports	Shows TCP/UDP ports.
connections	Shows network connections.

Example

The following command displays the server connections to your PX device.

```
diag>       netstat connections
```

Testing the Network Connectivity

This command syntax sends the ICMP ECHO_REQUEST message to a network host for checking its network connectivity. If the output shows the host is responding properly, the network connectivity is good, or the host is shut down or not being connected to the network.

```
diag>       ping <host>
```

Variables:

- <host> is the host name or IP address whose networking connectivity you want to check.

Options:

- You can include any or all of additional options listed below in the ping command.

Options	Description
count <number1>	Determines the number of messages to be sent. <number1> is an integer number.
size <number2>	Determines the packet size. <number2> is an integer number in bytes.
timeout <number3>	Determines the waiting period before timeout. <number3> is an integer number in seconds.

The command looks like this syntax when it includes all options:

```
diag>       ping <host> count <number1> size <number2> timeout <number3>
```

Example

The following command checks the network connectivity of the host 192.168.84.222 by sending the ICMP ECHO_REQUEST message to the host for 5 times.

```
diag>       ping 192.168.84.222 count 5
```

Tracing the Route

This command syntax traces the network route between your PX device and a network host.

```
diag>       traceroute <host>
```

Variables:

- <host> is the name or IP address of the host you want to trace.

Example

The following command displays the existing network routing for the host 192.168.84.222.

```
diag>       traceroute 192.168.84.222
```

Quitting the Diagnostic Mode

▶ **To quit the diagnostic mode, use this command:**

```
diag>       exit
```

The # prompt appears after pressing Enter, indicating that you have entered the administrator mode.

Retrieving Previous Commands

If you would like to retrieve any command that was previously typed in the same connection session, press the Up arrow (↑) on the keyboard until the desired command is displayed.

Automatically Completing a Command

A CLI command always consists of several words. You can easily enter a command by typing first word(s) or letter(s) and then pressing Tab or Ctrl+i instead of typing the whole command word by word.

▶ **To have a command completed automatically:**

1. Type initial letters or words of the desired command. Make sure the letters or words you typed are unique so that the CLI can identify the command you want.

2. Press Tab or Ctrl+i until the complete command appears.

Example 1:

Type the first word of the "`reset factorydefaults`" command, that is, `reset`. Then press Tab or Ctrl+i to make the rest of the command appears.

Example 2:

Type the first word and initial letters of the second word of the "`security enforceHttpsForWebAccess`" command, that is, `security enf`. Then press Tab or Ctrl+i to complete the second word.

Logging out of CLI

After completing your tasks using the CLI, always log out of the CLI to prevent others from accessing the CLI.

To log out of the CLI:

1. Ensure you have entered the administrator mode and the # prompt is displayed.
2. Type `exit` and press Enter.

Chapter 9 In-Line Monitors

The model name of a PX in-line monitor follows this format: PX2-3nnn, where n is a number, such as PX2-3172.

Unlike most of PX devices, each inlet of an in-line monitor is connected to an outlet only, so an inlet's rating is the same as an outlet's rating.

In This Chapter

Overview....448
Safety Instructions....448
Flexible Cord Installation Instructions....449
In-Line Monitor's LED Display....456
In-Line Monitor's Web Interface....457

Overview

An in-line monitor is implemented with the same number of inlets and outlets. An inlet is connected to a power source for receiving electricity, such as electric distribution panels or branch circuit receptacles. An outlet is connected to a device that draws power, such as a cooling or IT device.

Inlets are located at the side labeled **Line**, and outlets are located at the side labeled **Load**.

Safety Instructions

1. Installation of this product should only be performed by a licensed electrician.
2. Make sure the line cord is disconnected from power before physically mounting or moving the location of this product.
3. This product is intended to be located in an equipment rack in an information technology room. In the United States, installation must comply and be done in accordance with NEC (2011) Article 645 *Information Technology Equipment*.
4. This product is designed to be used within an electronic equipment rack. The metal case of this product is electrically bonded to the line cord ground wire. A threaded grounding point on the case may be used as an additional means of protectively grounding this product and the rack.
5. Examine the branch circuit receptacle that will supply electric power to this product. Make sure the receptacle’s power lines, neutral and protective earth ground pins are wired correctly and are the correct voltage and phase. Make sure the branch circuit receptacle is protected by a suitably rated fuse or circuit breaker.

6. If the product is a model that contains receptacles that can be switched on/off, electric power may still be present at a receptacle even when it is switched off.

Flexible Cord Installation Instructions

The following instructions are for Raritan products manufactured to accept user-installed flexible cords. These products are visually identified by the cable gland used to hold the flexible cord.

Important: Complete and the most updated instructions on installing a flexible cord on Raritan PDUs are included in the *Raritan PX Power Cord Installation Guide*, which is available on the Raritan website at this URL: http://www.raritan.com/support/dominion-px2/other-support-files/power-cord-installation-guide.

Flexible Cord Selection

- The preferred flexible cable is type SOOW, 600V, 90°C or 105°C. Consult Raritan before using a different flexible cable type.
- The rated ampacity of the flexible cord must be greater than or equal to the Raritan product's rated ampacity marked on its nameplate. In the United States, relevant ampacity ratings for flexible cords can be found in NEC(2011) section 400.5.
- The number of wires in the flexible cord must match the number of terminals (including the ground terminal) inside the Raritan product. See ***Wiring of 3-Phase In-Line Monitors*** (on page 451) for exceptions.
- If a plug is to be attached to the flexible cord, the length of the flexible cord must not exceed 4.5 meters - as specified in UL 60950-1 (2007) and NEC 645.5 (2011).
- The flexible cord may be permanently connected to power subject to local regulatory agency approval. In the United States, relevant electrical regulations can be found in NEC (2011) sections 400.7(A)(8), 400.7(B), 368.56 and table 400.4.

Plug Selection

If a plug is to be attached to the flexible cord, the plug's rated ampacity is chosen as follows:

- In the United States, as specified in UL 60950-1, the plug's rated ampacity must be 125% greater than the Raritan product's rated ampacity. In some Raritan products, such as 35A 3-phase delta wired PDUs, an exactly 125% rated plug is not available. In these cases, choose the closest plug that is more than 125%. For example, a 50A plug is the closest fit for a 35A 3-phase PDU.
- For all other locations, subject to local regulatory agency policy, the plug's rated ampacity is the same as the Raritan products rated ampacity.

Receptacle Selection

For Raritan in-line monitors, any receptacle fitted to the outlet flexible cord must have identical ratings as the plug attached to the inlet flexible cord.

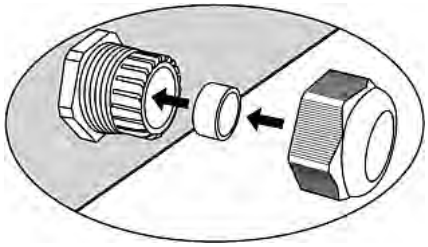
Derating a Raritan Product

Lower rated plugs, receptacles and flexible cords may be connected to a Raritan product. This results in a derated (reduced) ampacity rating for the product.

Derating guidelines:

1. Choose the plug and use its rated ampacity to determine the derated ampacity.
   - In the United States, as specified in UL 60950-1, the derated ampacity is 80% of the plug's rated ampacity. For example, a 30A plug would result in a derated ampacity of 24A.
   - In other geographic locations, subject to local regulatory agency approval, the derated ampacity is the plug's rated ampacity. For example, using a 16A plug would result in a derated ampacity of 16A.
2. The derated ampacity must be marked on the Raritan product so the new reduced rating can be easily identified.
3. For in-line monitors, the receptacles used must have the same voltage and ampacity rating as the plug chosen in step 1.

4. The flexible cord must have a rated ampacity greater than or equal to the derated ampacity. Since the new flexible cord may be smaller diameter, a check must be performed to insure the cable gland nut, when tightened, will securely hold the flexible cord so that it cannot be twisted, pulled or pushed in the cable gland. A sealing ring, for small diameter flexible cords, may have been included with the Raritan product, or one can be requested from Raritan, to reduce the inside diameter of the cable gland.



Wiring of 3-Phase In-Line Monitors

3-phase in-line monitors contain 4-pole wiring terminal blocks (L1, L2, L3, N) to monitor 5-wire (4P+PE) 3-phase wye connections. Delta wired 4-wire (3P+PE) 3-phase connections are also permitted (no wire connected to the terminal block neutral “N”). No additional hardware or firmware configuration is required to specify whether the connection is 5-wire wye or 4-wire delta.

In-Line Monitor Unused Channels

It is not necessary to wire up all channels of multi-channel in-line monitors. The inlet and outlet openings of unused channels must be completely closed off. “Goof plugs” for this purpose may be a good choice if they are available in your country or region.

Step by Step Flexible Cord Installation

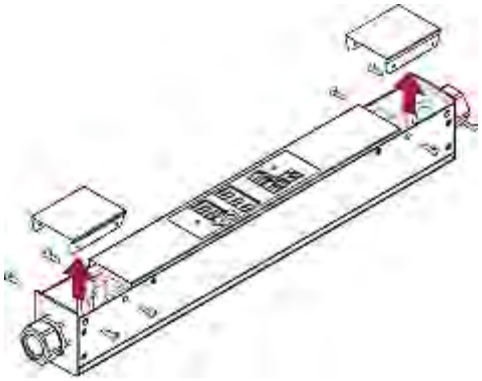
The following items are required to complete the installation:

- Flexible cord(s).
- Insulated ring terminals (one for each wire) and appropriate crimp tool.
- Plug(s) and receptacle(s) (for in-line monitors)
- Torque screwdriver, torque nut driver and torque wrench to tighten the wiring terminal block screws, ground nut and cable gland nut.

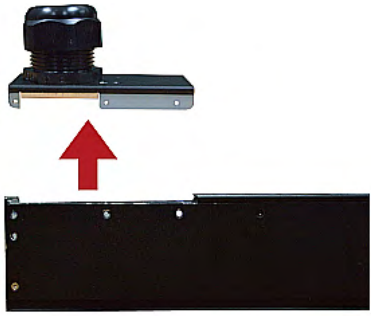
▶ To install a flexible cord:

1. Open the PDU's access panel (or in-line monitor top panel) to expose the power wiring terminal block(s).

One-channel in-line monitor

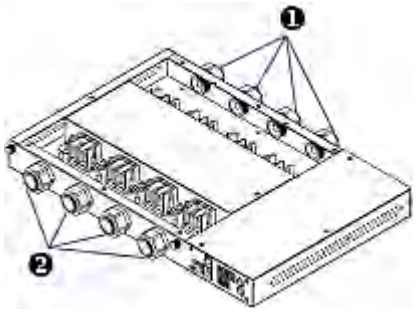


Zero U PDU



Make sure to locate the ground wire mounting stud(s). There is a separate ground wire mounting stud for each terminal block. Each flexible cord MUST have its green (or green/yellow) ground wire bonded to a ground wire mounting stud.

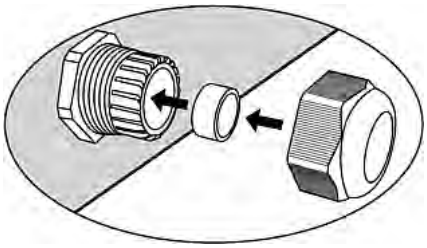
For in-line monitors, make sure to identify the inlet terminal blocks (rear of monitor) and outlet terminal blocks (front of monitor). Each inlet terminal block has a corresponding outlet terminal block.



Number	Description
❶	Inlets (labeled LINE)
❷	Outlets (labeled LOAD)

2. Strip off the outer jacket of the flexible cord and remove any jute, paper or other fillers. Use the following to help determine how much jacket to remove:
   - In the finished assembly, the outer jacket should protrude inside the Raritan product.
   - The wires will have ring terminals crimped onto them.
   - In the finished assembly, the wires should have some slack and not be taught.
   - In the finished assembly, if the flexible cord slips in the cable gland placing a strain on the cord's wires, the ground wire must be the last wire to take the strain.
3. Crimp an insulated ring terminal onto each wire. A non-insulated ring terminal may be used for the ground wire. Inspect each crimp to insure it is secure and verify no exposed wire protrudes from the rear of an insulated ring terminal.
4. Loosen the cable gland nut and push the flexible cord assembly through the gland.

Temporarily hand tighten the gland nut and verify the cord cannot be twisted or pushed or pulled in the gland. Do not proceed if hand tightening results in a loose cord. In some models, especially in-line monitors, the flexible cord's diameter may be too small for the cable gland. A sealing ring for smaller diameter line cords may have been included with the Raritan product, or can be requested from Raritan, to reduce the inside diameter of the cable gland.



5. Fasten the ring terminal of the green (or green/yellow) ground wire to the chassis's threaded ground stud in this order:
   a. Place the lock washer on the stud.
   b. Place the ground wire ring terminal on the stud.
   c. Place the nut on the stud and tighten with a torque wrench. The appropriate torque settings vary according to the nut size.

Nut size	Torque setting (N·m)	Tolerance
M3	0.49	10%
M4	1.27	8%
M5	1.96	5%
M6	2.94	3.5%
M8	4.9	2%

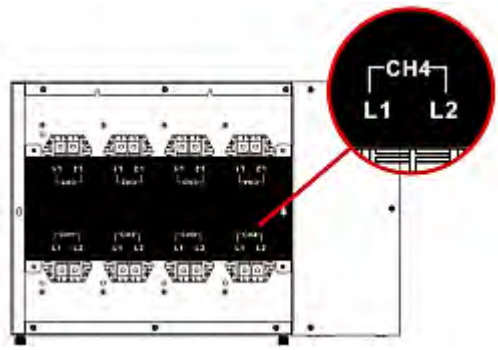
   d. Check the ground wire connection. It should be secure and not move or rotate.

6. Fasten the ring terminals of all remaining wires to the terminal block and tighten each using a torque screwdriver. The appropriate torque settings vary according to the screw size.

Screw size	Torque setting (N·m)	Tolerance
M3	0.49	10%
M4	1.27	8%
M5	1.96	5%
M6	2.94	3.5%
M8	4.9	2%

Make sure each ring terminal is firmly fastened and cannot be twisted by hand. Use the following guidelines to help terminal block wiring.

- In single-phase Raritan products with world-wide ratings, the terminals are labeled L1 and L2. L1 is the phase wire. L2 is either the neutral (120/230V installations) or another phase wire (208V installations).



- In all 3-phase products, L1 is phase A, L2 is phase B, L3 is phase C and N is neutral.
- For Raritan in-line monitors, where there is a one to one correspondence between plug and receptacle, maintain the same wire colors for inlet and outlet flexible cords.

7. Make final adjustments to the cable gland and verify the jacket of the flexible cord extends into the Raritan product. Hand tighten the gland nut and finish tightening with a torque wrench. Appropriate torque settings vary according to the cable gland size.

Cable gland size	Torque setting (N·m)
M12x1.5	0.7 to 0.9
M16x1.5	2.0 to 3.0
M20x1.5	2.7 to 4.0

Cable gland size	Torque setting (N·m)
M25x1.5	5.0 to 7.5
M32x1.5	7.5 to 10.0
M40x1.5	7.5 to 10.0
M50x1.5	7.5 to 10.0
M63x1.5	7.5 to 10.0

Note: The cable gland size is marked on the cable gland body.

After tightening, examine the flexible cord and cable gland for the following:

- Make sure you can see a few remaining threads between the cable gland body and cable gland nut. The gland nut must not bottom out on the gland body.
- Make sure the flexible cord does not move in the cable gland when it is twisted, pushed or pulled.

8. Re-install the PDU wiring access panel or in-line monitor cover plate. This completes internal wiring of the Raritan product.
9. For in-line monitors, fasten the receptacles to the outlet flexible cords following the manufacturer's instructions.
10. Complete the wiring of the inlet flexible cord by performing one of these steps:
    - Assemble the plug following the manufacturer's instructions.
    - Permanently attach and strain relief the flexible cord to a junction box following applicable electrical codes.

In-Line Monitor's LED Display

The LED display of an in-line monitor is the same as a regular PX model. See ***LED Display*** (on page 65).

Automatic Mode

Unlike regular PX models, the in-line monitor's LED display only cycles through the current readings of each outlet in the Automatic Mode.

Manual Mode

You can switch between voltage, active power and current readings of the selected outlet in the Manual Mode on an in-line monitor. To enter the Manual Mode, press the Up or Down button.

To operate the LED display of an inline monitor:

1. Press the Up or Down button until the desired outlet number is selected in the two-digit row.
   - Pressing the Up button moves up one selection.
   - Pressing the Down button moves down one selection.

   If your inline monitor has only one outlet, go to Step 2.
2. Current of the selected outlet is shown in the three-digit row. Simultaneously the CURRENT(A) LED is lit. See ***LEDs for Measurement Units*** (on page 67).
3. If desired, you can press the Up and Down buttons simultaneously to switch between voltage, active power and current readings.
   - The voltage appears in this format: XXX (V). It is displayed for about five seconds, after which the current reading re-appears. When the voltage is displayed, the VOLTAGE(V) LED is lit.
   - The active power appears in one of the formats: X.XX, XX.X, and XXX (kW). It is displayed for about five seconds, after which the current reading re-appears. When the active power is displayed, the POWER(kW) LED is lit.
4. While the final outlet's active power is being displayed, you can press the Up button to show the first outlet's unbalanced load. The UB LOAD (%) LED is lit.
   - Then press the Up and Down buttons to switch between different outlet's unbalanced load readings if there are more than one outlet.

Note: The LED display returns to the Automatic Mode after 20 seconds elapse since the last time any button was pressed.

In-Line Monitor's Web Interface

An in-line monitor's web interface is similar to a regular PX model's web interface.

See ***Using the Web Interface*** (on page 77) for login instructions and additional information.

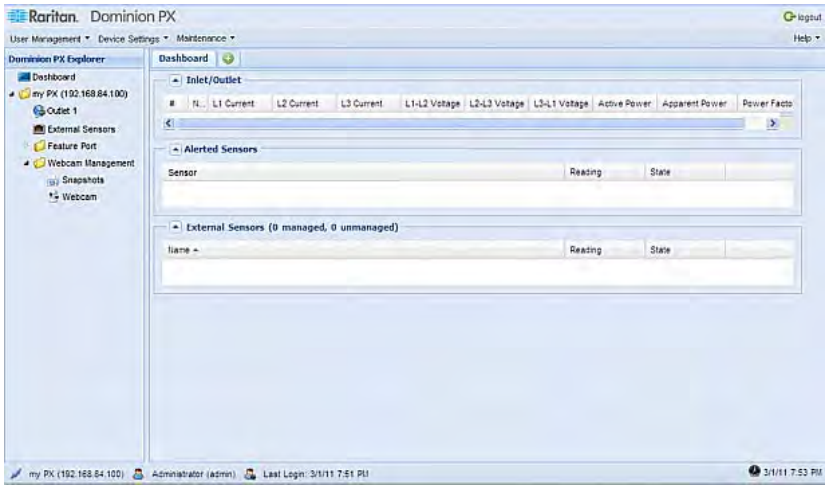
Dashboard Page

After login, the web interface displays the Dashboard page by default. An inline monitor's Dashboard page looks slightly different from a regular PX device's Dashboard page.

The power status of the outlet on a three-phase Y-wired inline monitor is displayed on this page, including:

- Current of L1, L2 and L3
- Voltage of L1-L2, L2-L3, and L3-L1
- Active power
- Apparent power
- Power factor

Note: Depending on your model, elements shown on the same page may appear slightly different from this image.



Outlet Page

An inline monitor's Outlet page displays more information than a regular PX device's Outlet page, including:

- Current per outlet

  Current per line (for a three-phase model)
- Voltage per outlet

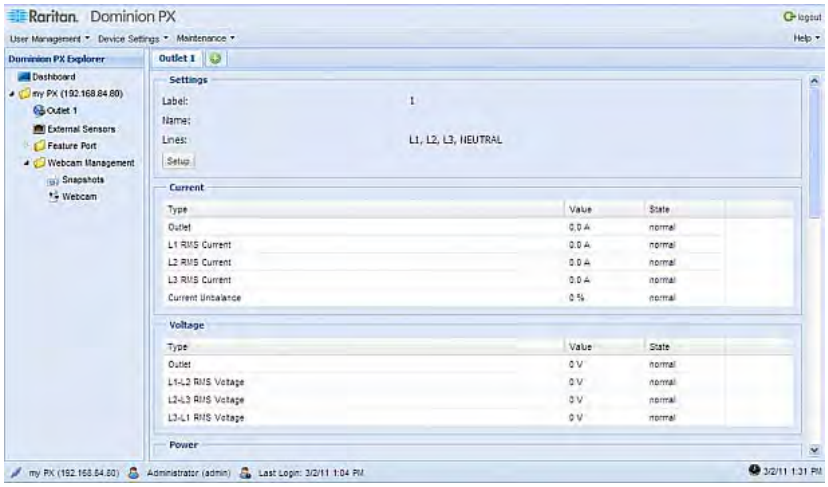
  Voltage per line (for a three-phase model)
- Power-related readings per outlet

  Power-related readings per line (for a three-phase model)

- Threshold settings per outlet

  Threshold settings per line (for a three-phase model)

Note: Depending on your model, elements shown on the same page may appear slightly different from this image.



Appendix A Specifications

In This Chapter

Power Measurement Accuracy 460
Maximum Ambient Operating Temperature 460
Serial RS-232 Port Pinouts.....461
Sensor RJ-12 Port Pinouts.....461
Feature RJ-45 Port Pinouts.....461

Power Measurement Accuracy

The following measurement accuracy applies to all Raritan PDUs whose model names begin with PX2 or PXE.

	Power measurement accuracy	Measurement accuracy range
RMS voltage (V)	1%	
RMS current (A)	1%+/-0.1A	0.1A to rated current
Active power (Watts)	1%	20W to rated power
Apparent power (VA)	1%	20VA to rated power
Active energy (Watts-hour)	1%	

Maximum Ambient Operating Temperature

The maximum ambient operating temperature (TMA) for PX varies from 50 to 60 degrees Celsius, depending on the model and certification standard (CE or UL). If necessary, contact Raritan Technical Support for this information for your model.

Specification	Measure
Max Ambient Temperature	50 to 60 degrees Celsius

Serial RS-232 Port Pinouts

RS-232 Pin/signal definition			
Pin No.	Signal	Direction	Description
1	DCD	Input	Data
2	RxD	Input	Receive data (data in)
3	TxD	Output	Transmit data
4	DTR	Output	Data terminal ready
5	GND	—	Signal ground
6	DSR	Input	Data set ready
7	RTS	Output	Request to send
8	CTS	Input	Clear to send
9	RI	Input	Ring indicator

Sensor RJ-12 Port Pinouts

RJ-12 Pin/signal definition			
Pin No.	Signal	Direction	Description
1	+12V	—	Power (500mA, fuse protected)
2	GND	—	Signal Ground
3	—	—	—
4	—	—	—
5	GND	—	Signal Ground
6	1-wire		Used for Feature Port

Feature RJ-45 Port Pinouts

RJ-45 Pin/signal definition			
Pin No.	Signal	Direction	Description
1	DTR	Output	Reserved
2	GND	—	Signal Ground

RJ-45 Pin/signal definition			
Pin No.	Signal	Direction	Description
3	+5V	—	Power for CIM (200mA, fuse protected) Warning: Pin 3 is only intended for use with Raritan devices.
4	TxD	Output	Transmit Data (Data out)
5	RxD	Input	Receive Data (Data in)
6	N/C	N/C	No Connection
7	GND	—	Signal Ground
8	DCD	Input	Reserved

Appendix B Equipment Setup Worksheet

PX Series Model _____

PX Series Serial Number _____

OUTLET 1	OUTLET 2	OUTLET 3
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 4	**OUTLET 5**	**OUTLET 6**
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE

OUTLET 7	OUTLET 8	OUTLET 9
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 10	OUTLET 11	OUTLET 12
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 13	OUTLET 14	OUTLET 15
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE

OUTLET 16	OUTLET 17	OUTLET 18
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE
OUTLET 19	OUTLET 20	OUTLET 21
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE

OUTLET 22	OUTLET 23	OUTLET 24
MODEL	MODEL	MODEL
SERIAL NUMBER	SERIAL NUMBER	SERIAL NUMBER
USE	USE	USE

Types of adapters

_____

Types of cables

_____

Name of software program

_____

Appendix C Resetting to Factory Defaults

For security reasons, the PX device can be reset to factory defaults only at the local console.

Important: Exercise caution before resetting the PX to its factory defaults. This erases existing information and customized settings, such as user profiles, threshold values, and so on. Only active energy data and firmware upgrade history are retained forever.

You can use either the reset button or the command line interface (CLI) to reset the PX.

In This Chapter

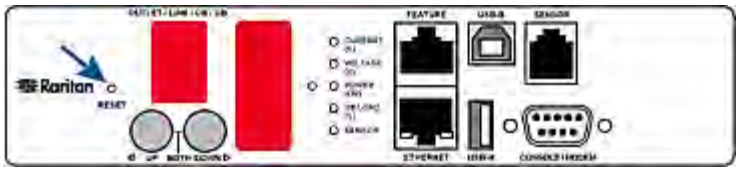
Using the Reset Button.....467
Using the CLI Command 468

Using the Reset Button

To reset to factory defaults using the reset button:

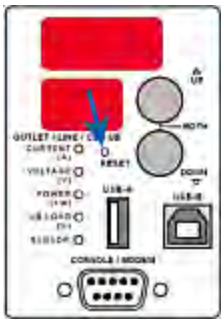
1. Connect a computer to the PX device. See ***Connecting the PX to a Computer*** (on page 17).
2. Launch a terminal emulation program such as HyperTerminal, Kermit, or PuTTY, and open a window on the PX. For information on the serial port configuration, see Step 2 of ***Initial Network Configuration*** (on page 22).
3. Press (and release) the Reset button of the PX device while pressing the Esc key of the keyboard several times in rapid succession. A prompt (=>) should appear after about one second.
4. Type *defaults* to reset the PX to its factory defaults.
5. Wait until the Username prompt appears, indicating the reset is complete.

This diagram shows the location of the reset button on Zero U models.



This diagram shows the location of the reset button on 1U models.

This diagram shows the location of the reset button on 2U models.



Note: HyperTerminal is available on Windows operating systems prior to Windows Vista. For Windows Vista or later versions, you may use PuTTY, which is a free program you can download from the Internet. See PuTTY's documentation for details on configuration.

Using the CLI Command

The Command Line Interface (CLI) provides a reset command for restoring the PX to factory defaults. For information on CLI, see ***Using the Command Line Interface*** (on page 273).

To reset to factory defaults using the CLI command:

1. Connect a computer to the PX device. See ***Connecting the PX to a Computer*** (on page 17).
2. Launch a terminal emulation program such as HyperTerminal, Kermit, or PuTTY, and open a window on the PX. For information on the serial port configuration, see Step 2 of ***Initial Network Configuration*** (on page 22).

3. Log in to the CLI by typing the user name "admin" and its password. See Step 4 of ***Initial Network Configuration*** (on page 22).
4. After the # system prompt appears, type either of the following commands and press Enter.

   ```
   #     reset factorydefaults
   ```

   -- OR --

   ```
   #     reset factorydefaults /y
   ```

5. If you entered the command without "/y" in Step 4, a message appears prompting you to confirm the operation. Type y to confirm the reset.
6. Wait until the Username prompt appears, indicating the reset is complete.

To reset to factory defaults without logging in to the CLI:

As of release 2.4, the PX provides an easier way to reset the product to factory defaults in the CLI prior to login.

1. Connect a computer to the PX and launch a terminal emulation program as described in the above procedure.
2. At the Username prompt in the CLI, type "factorydefaults" and press Enter.

   ```
   Username:  factorydefaults
   ```

3. Type y on a confirmation message to perform the reset.

Appendix D LDAP Configuration Illustration

This section provides an LDAP example for illustrating the configuration procedure using Microsoft Active Directory® (AD). To configure LDAP authentication, four main steps are required:

a. Determine user accounts and groups intended for the PX

b. Create user groups for the PX on the AD server

c. Configure LDAP authentication on the PX device

d. Configure roles on the PX device

In This Chapter

Step A. Determine User Accounts and Groups 470
Step B. Configure User Groups on the AD Server 471
Step C. Configure LDAP Authentication on the PX Device 472
Step D. Configure User Groups on the PX Device 474

Step A. Determine User Accounts and Groups

Determine the user accounts and groups that are authenticated for accessing the PX. In this example, we will create two user groups with different permissions. Each group will consist of two user accounts available on the AD server.

User groups	User accounts (members)
PX_User	usera
	pxuser2
PX_Admin	userb
	pxuser

Group permissions:

- The PX_User group will have neither system permissions nor outlet permissions.
- The PX_Admin group will have full system and outlet permissions.

Step B. Configure User Groups on the AD Server

You must create the groups for the PX on the AD server, and then make appropriate users members of these groups.

In this illustration, we assume:

- The groups for the PX are named *PX_Admin* and *PX_User*.
- User accounts *pxuser*, *pxuser2*, *usera* and *userb* already exist on the AD server.

To configure the user groups on the AD server:

1. On the AD server, create new groups -- *PX_Admin* and *PX_User*.

   Note: See the documentation or online help accompanying Microsoft AD for detailed instructions.

2. Add the *pxuser2* and *usera* accounts to the PX_User group.
3. Add the *pxuser* and *userb* accounts to the PX_Admin group.
4. Verify whether each group comprises correct users.

Step C. Configure LDAP Authentication on the PX Device

You must enable and set up LDAP authentication properly on the PX device to use external authentication.

In the illustration, we assume:

- The DNS server settings have been configured properly. See ***Modifying the Network Settings*** (on page 101) and ***Role of a DNS Server*** (on page 105).
- The AD server's domain name is *techadssl.com*, and its IP address is *192.168.56.3*.
- The AD protocol is NOT encrypted over SSL.
- The AD server uses the default TCP port *389*.
- Anonymous bind is used.

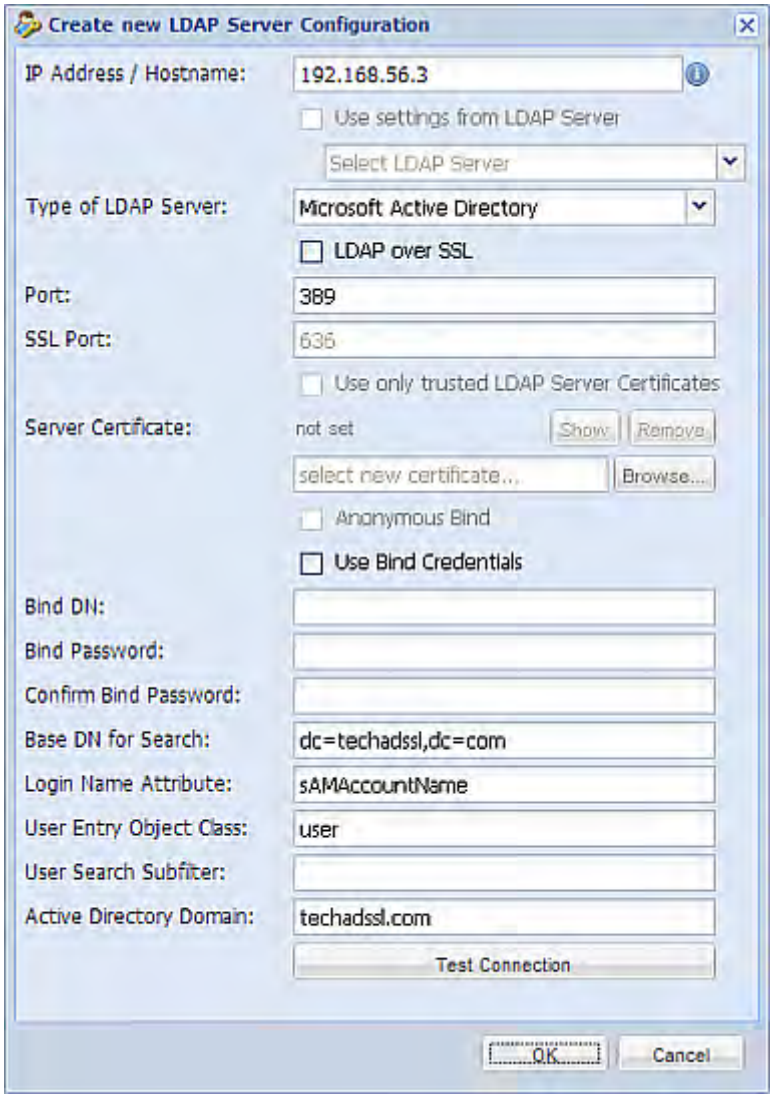
To configure LDAP authentication:

1. Choose Device Settings > Security > Authentication. The Authentication Settings dialog appears.
2. Select the LDAP radio button to activate remote LDAP/LDAPS server authentication.
3. Click New to add an LDAP/LDAPS server for authentication. The "Create new LDAP Server Configuration" dialog appears.
4. Provide the PX with the information about the AD server.
   - IP Address / Hostname - Type the domain name `techadssl.com` or IP address `192.168.56.3`.

   Important: Without the SSL encryption enabled, you can type either the domain name or IP address in this field, but you must type the fully qualified domain name if the SSL encryption is enabled.

   - Use settings from LDAP server - Leave the checkbox deselected.
   - Type of LDAP Server - Select "Microsoft Active Directory" from the drop-down list.
   - LDAP over SSL - Have the checkbox deselected since the SSL encryption is not applied in this example.
   - Port - Ensure the field is set to 389.
   - SSL Port and Server Certificate - Skip the two fields since the SSL encryption is not enabled.
   - Use Bind Credentials - Do NOT select this checkbox because anonymous bind is used.
   - Bind DN, Bind Password and Confirm Bind Password -- Skip the three fields because anonymous bind is used.

- Base DN for Search - Type `dc=techadssl,dc=com` as the starting point where your search begins on the AD server.
- Login Name Attribute - Ensure the field is set to `sAMAccountName` because the LDAP server is Microsoft Active Directory.
- User Entry Object Class - Ensure the field is set to `user` because the LDAP server is Microsoft Active Directory.
- User Search Subfilter - The field is optional. The subfilter information is also useful for filtering out additional objects in a large directory structure. In this example, we leave it blank.
- Active Directory Domain - Type `techadssl.com`.



5. Click OK to save the changes. The LDAP server is saved.

6. Click OK to save the changes. The LDAP authentication is activated.

Note: If the PX clock and the LDAP server clock are out of sync, the certificates are considered expired and users are unable to authenticate using LDAP. To ensure proper synchronization, administrators should configure the PX and the LDAP server to use the same NTP server.

Step D. Configure User Groups on the PX Device

A role on the PX device determines the system and outlet permissions. You must create the roles whose names are identical to the user groups created for the PX on the AD server or authorization will fail. Therefore, we will create the roles named *PX_User* and *PX_Admin* on the PDU.

In this illustration, we assume:

- Users assigned to the *PX_User* role can neither configure PX nor access the outlets.
- Users assigned to the *PX_Admin* role have the Administrator permissions so they can both configure PX and access the outlets.

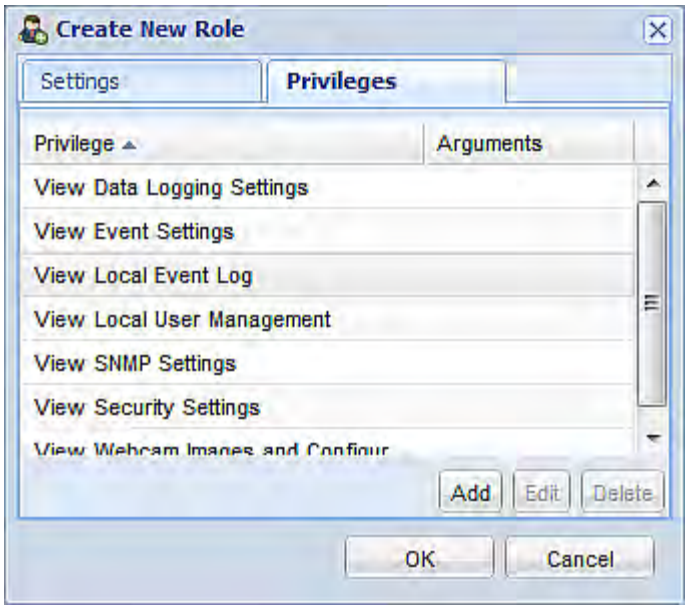
To create the PX_User role with appropriate permissions assigned:

1. Choose User Management > Roles. The Manage Roles dialog appears.

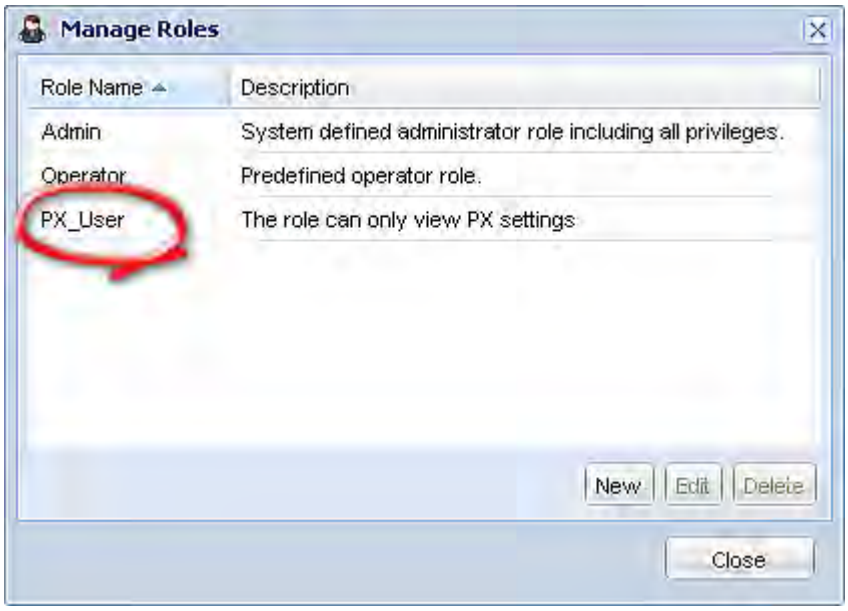
   Tip: You can also access the Manage Roles dialog by clicking the Manage Roles button in the Edit User 'XXX' dialog.

2. Click New. The Create New Role dialog appears.
3. Type `PX_User` in the Role Name field.
4. Type a description for the PX_User role in the Description field. In this example, we type "The role can only view PX settings" to describe the role.
5. Click the Privileges tab to select all View XXX permissions (where XXX is the name of the setting). A View XXX permission lets users view the XXX settings without the capability to configure or change them.
   a. Click Add. The "Add Privileges to new Role" dialog appears.
   b. Select a permission beginning with the word "View" from the Privileges list, such as View Event Settings.
   c. Click Add.

d. Repeat Steps a to c to add all permissions beginning with "View."



6. Click OK to save the changes. The PX_User role is created.

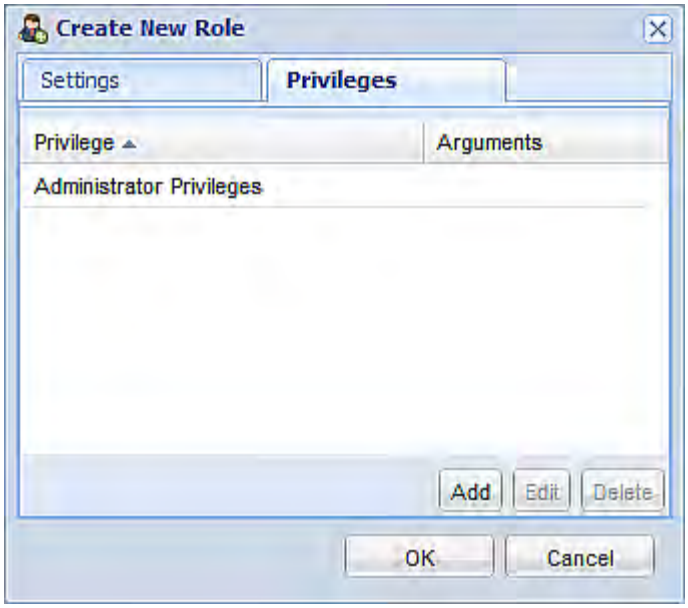


7. Keep the Manage Roles dialog opened to create the PX_Admin role.

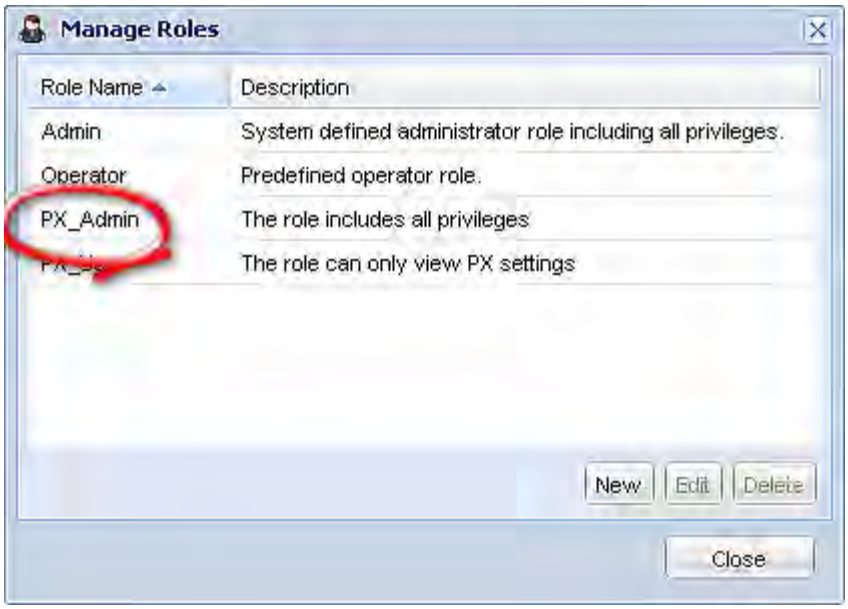
To create the PX_Admin role with full permissions assigned:

1. Click New. The Create New Role dialog appears.
2. Type `PX_Admin` in the Role Name field.

3. Type a description for the PX_Admin role in the Description field. In this example, we type "The role includes all privileges" to describe the role.
4. Click the Privileges tab to select the Administrator permission. The Administrator permission allows users to configure or change all PX settings.
   a. Click Add. The "Add Privileges to new Role" dialog appears.
   b. Select the permission named Administrator Privileges from the Privileges list.
   c. Click Add.



5. Click OK to save the changes. The PX_Admin role is created.



6. Click Close to quit the dialog.

Appendix E Integration

The PX device can work with certain Raritan or non-Raritan products to provide diverse power solutions.

In This Chapter

Power IQ Configuration 478
Dominion KX II Configuration 480
Dominion KSX II or SX Configuration.....484
dcTrack.....492
RF Code Energy Monitoring Solution.....495

Power IQ Configuration

Raritan's Power IQ is a software application that collects and manages the data from different PDUs installed in your server room or data center. With this software, you can:

- Do bulk configuration for multiple PDUs
- Name outlets on different PDUs
- Switch on/off outlets on outlet-switching capable PDUs

For more information on Power IQ, see either of the following:

- Power IQ User Guide: Available on the Raritan website's ***Firmware and Documentation section*** (***http://www.raritan.com/support/firmware-and-documentation/***).
- Power IQ Online Help: Available on the ***Product Online Help section*** (***http://www.raritan.com/support/online-help/***).

Adding PDUs to Power IQ Management

Once Power IQ is configured, add Raritan PX or other PDUs to its management. Power IQ can then gather data from these PDUs.

You can also add PDUs to Power IQ by uploading a CSV file containing the information. See Adding PDUs in Bulk with CSV Files in the Power IQ User Guide.

Use this procedure to add a Raritan EMX to Power IQ.

To add PDUs to Power IQ management:

1. In the PDUs tab, click Add.
2. Enter the IP address of the PDU.

3. If the PDU is in a daisy-chained configuration or console server configuration, enter the PDU's position number in the chain or serial port number in the Proxy Index field. You can also specify branch circuit monitors using the Proxy Index field. See Adding Veris Branch Circuit Monitors with Acquisuite.

   Note: If the PDU is not in this type of configuration, leave the Proxy Index field blank.

4. Enter an asset tag number or other asset management code in the External Key field. **Optional.**
5. Enter data in Custom Field 1 and Custom Field 2. **Optional.** The labels may have been changed in Power IQ to identify these fields.
6. If the PDU is a Raritan PX, enter a valid Username and Password for the PDU in the PDU Administrative Credentials section. Re-enter the password in the Password Confirm field.
7. Select the SNMP Version.
   - For SNMP version 1/2c PDUs, enter an SNMP Community String that has at least READ permissions to this PDU. This enables polling the PDU for data. Enter an SNMP community string that has both READ and WRITE permissions to the PDU to enable power control, outlet renaming, and buffered data retrieval.
   - For SNMP version 3 PDUs, enter the Username and select an Authorization Level. The authorization levels are:
     - noAuthNoPriv - No Authentication Passkey, No Encoding Passkey
     - authNoPriv - Authentication Passkey, No Encoding Passkey
     - authPriv - Authentication Passkey, Encoding Passkey

   a. Depending on the Authorization Level selected, you must enter additional credentials for Authorization and Privacy.
   b. Authorization Protocol: Select MD5 or SHA.
   c. Enter the PDU's Authorization Passkey, then re-enter the passkey in the Authorization Passkey Confirm field.
   d. Privacy Protocol: Select DES or AES.
   e. Enter the PDU's Privacy Passkey, then re-enter the passkey in the Privacy Passkey Confirm field.

   Note: You must enable the SNMP agent on all PDUs added to Power IQ.

8. Select "Validate and wait for discovery to complete before proceeding" to check credentials and view the discovery process status as you add this PDU. **Optional.** See Validating PDU Credentials in the Power IQ User Guide.
9. Click Add.

Note: PDU discovery is complete once the PDU model type is determined. SNMP fields such as contact or location values are not determined until this device is polled for the first time.

Once added, the PDU appears in the PDU list. Power IQ begins polling the PDU for sensor data. You can configure how often Power IQ polls PDU. See Configuring Polling Intervals in the Power IQ User Guide.

Dominion KX II Configuration

PX2 series PDUs can be connected to the Raritan's Dominion KX II device (a digital KVM switch) to provide one more alternative of power control.

Note that this integration requires the following firmware versions:

- Dominion KX II -- 2.4 or later
- PX2 series -- 2.2 or later

Dominion KX II integration requires D2CIM-PWR and straight CAT5 cable.

For more information on Dominion KX II, see either of the following:

- Dominion KX II User Guide: Available on the Raritan website's ***Firmware and Documentation section*** (***http://www.raritan.com/support/firmware-and-documentation/***).
- Dominion KX II Online Help: Available on the ***Product Online Help section*** (***http://www.raritan.com/support/online-help/***).

Configuring Rack PDU (Power Strip) Targets

The KX II allows you to connect rack PDUs (power strips) to KX II ports. KX II rack PDU configuration is done from the KX II Port Configuration page.

Note: Raritan recommends no more than eight (8) rack PDUs (power strips) be connected to a KX II at once since performance may be affected.

Connecting a Rack PDU

Rack PDUs are connected to the KX II using the D2CIM-PWR CIM.

To connect the rack PDU:

1. Connect the male RJ-45 of the D2CIM-PWR to the female RJ-45 connector labeled "FEATURE" of the rack PDU.
2. Connect the female RJ-45 connector of the D2CIM-PWR to any of the available female system port connectors on the KX II using a straight through Cat5 cable.

3. Attach an AC power cord to the target server and an available rack PDU outlet.
4. Connect the rack PDU to an AC power source.
5. Power on the device.

Naming the Rack PDU in the KX II or LX (Port Page for Power Strips)

Note: PX rack PDUs (power strips) can be named in the PX as well as in KX II and LX.

Once a Raritan remote rack PDU is connected to the KX II or LX, it will appear on the Port Configuration page. Click on the power port name on that page to access it. The Type and the Name fields are prepopulated.

Note: The (CIM) Type cannot be changed.

The following information is displayed for each outlet on the rack PDU: [Outlet] Number, Name, and Port Association.

Use this page to name the rack PDU and its outlets. Names can be up to 32 alphanumeric characters and can include special characters.

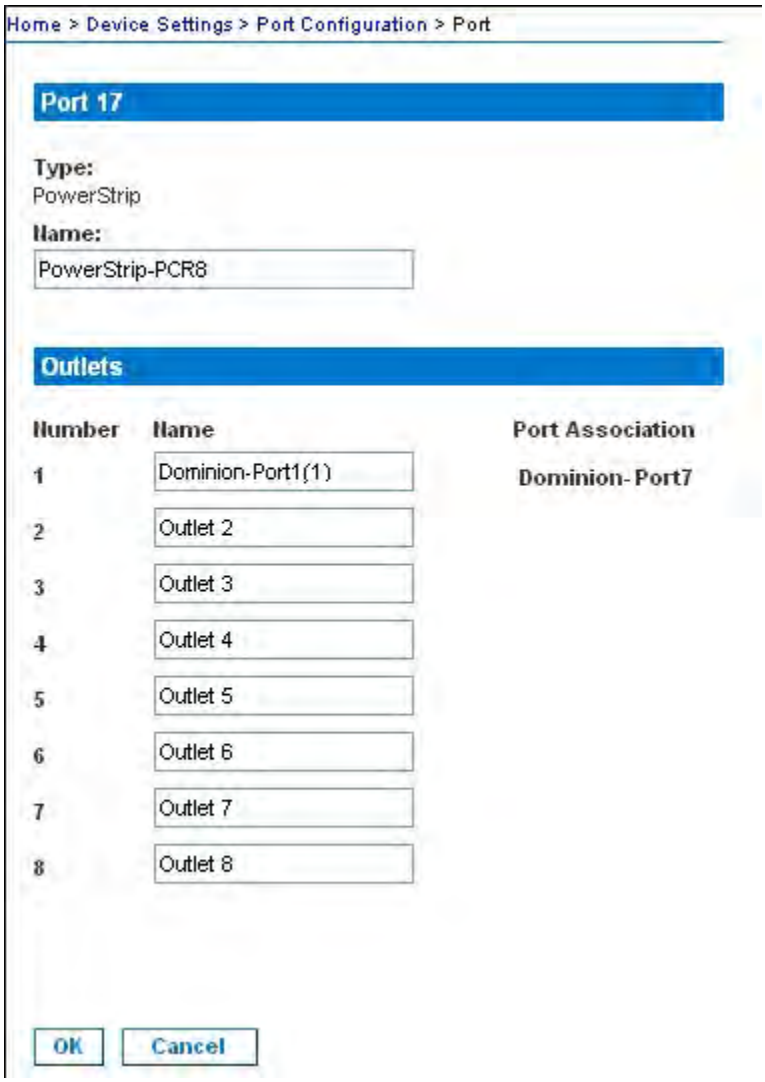
Note: When a rack PDU is associated with a target server (port), the outlet name is replaced by the target server name, even if you assigned another name to the outlet.

▶ To name the rack PDU and outlets:

Note: CommandCenter Secure Gateway does not recognize rack PDU names containing spaces.

1. Enter the Name of the rack PDU (if needed).
2. Change the [Outlet] Name if desired. (Outlet names default to the outlet #.)

3. Click OK.


Home > Device Settings > Port Configuration > Port
Port 17
Type:
PowerStrip
Name:
PowerStrip-PCR8
Outlets
Number
Name
Port Association
1
Dominion-Port1(1)
Dominion- Port7
2
Outlet 2
3
Outlet 3
4
Outlet 4
5
Outlet 5
6
Outlet 6
7
Outlet 7
8
Outlet 8
OK
Cancel

Associating Outlets with Target Servers on KX II and LX

The Port page opens when you click on a port on the Port Configuration page. From this page, you can make power associations, change the port name to something more descriptive, and update target server settings if you are using the D2CIM-VUSB CIM. The (CIM) Type and the (Port) Name fields are prepopulated; note that the CIM type cannot be changed.

A server can have up to four power plugs and you can associate a different rack PDU (power strip) with each. From this page, you can define those associations so that you can power on, power off, and power cycle the server from the Port Access page.

To use this feature, you will need:

- Raritan remote rack PDU(s)
- Power CIMs (D2CIM-PWR)

To make power associations (associate rack PDU outlets to KVM target servers):

Note: When a rack PDU is associated to a target server (port), the outlet name is replaced by the target server name (even if you assigned another name to the outlet).

1. Choose the rack PDU from the Power Strip Name drop-down list.
2. For that rack PDU, choose the outlet from the Outlet Name drop-down list.
3. Repeat steps 1 and 2 for all desired power associations.
4. Click OK. A confirmation message is displayed.

To change the port name:

1. Type something descriptive in the Name field. For example, the name of the target server would be a likely candidate. The name can be up to 32 alphanumeric characters and can include special characters.
2. Click OK.

Removing Power Associations

When disconnecting target servers and/or rack PDUs from the device, all power associations should first be deleted. When a target has been associated with a rack PDU and the target is removed from the device, the power association remains. When this occurs, you are not able to access the Port Configuration for that disconnected target server in Device Settings so that the power association can be properly remove.

To remove a rack PDU association:

1. Select the appropriate rack PDU from the Power Strip Name drop-down list.

2. For that rack PDU, select the appropriate outlet from the Outlet Name drop-down list.
3. From the Outlet Name drop-down list, select None.
4. Click OK. That rack PDU/outlet association is removed and a confirmation message is displayed.

To remove a rack PDU association if the rack PDU has been removed from the target:

1. Click Device Settings > Port Configuration and then click on the active target.
2. Associate the active target to the disconnected power port. This will break the disconnected target's power association.

Finally, associate the active target to the correct power port.

Dominion KSX II or SX Configuration

The PX2 series PDU supports the integration with Raritan's Dominion KSX II or SX serial access products as of release 2.4.

Different cables are needed when connecting to different Raritan access products.

- Use a Category 5 cable to connect from the PDU (power control) port of the Dominion KSX II to the FEATURE port of the PX.
- Use a CSCSPCS cable to connect from the PDU port of the Dominion SX to the FEATURE port of the PX.

Note: To only access the CLI of the PX via the SX, you can treat the PX as a serial device by connecting to the PDU's serial port instead of the FEATURE port.

For more information on either Raritan serial access product, see either of the following:

- Dominion KSX II or SX User Guide: Available on the Raritan website's ***Firmware and Documentation section*** (***http://www.raritan.com/support/firmware-and-documentation/***).
- Dominion KSX II or SX Online Help: Available on the ***Product Online Help section*** (***http://www.raritan.com/support/online-help/***).

Dominion KSX II

After connecting a Dominion KSX II to the PX, you can monitor the PDU and even control its outlets if the PDU is an outlet-switching capable model.

Overview

The KSX II allows you to control Raritan PX and RPC series rack PDU (power strip) outlets. Once a PX or RPC series is setup and then attached to the KSX II, the rack PDU and its outlets can be controlled from the Powerstrip page in the KSX II interface. This page is accessed by clicking on the Power menu at the top of the page.

The Powerstrip page will display rack PDUs attached to the KSX II for which the user has been granted appropriate port access permissions.

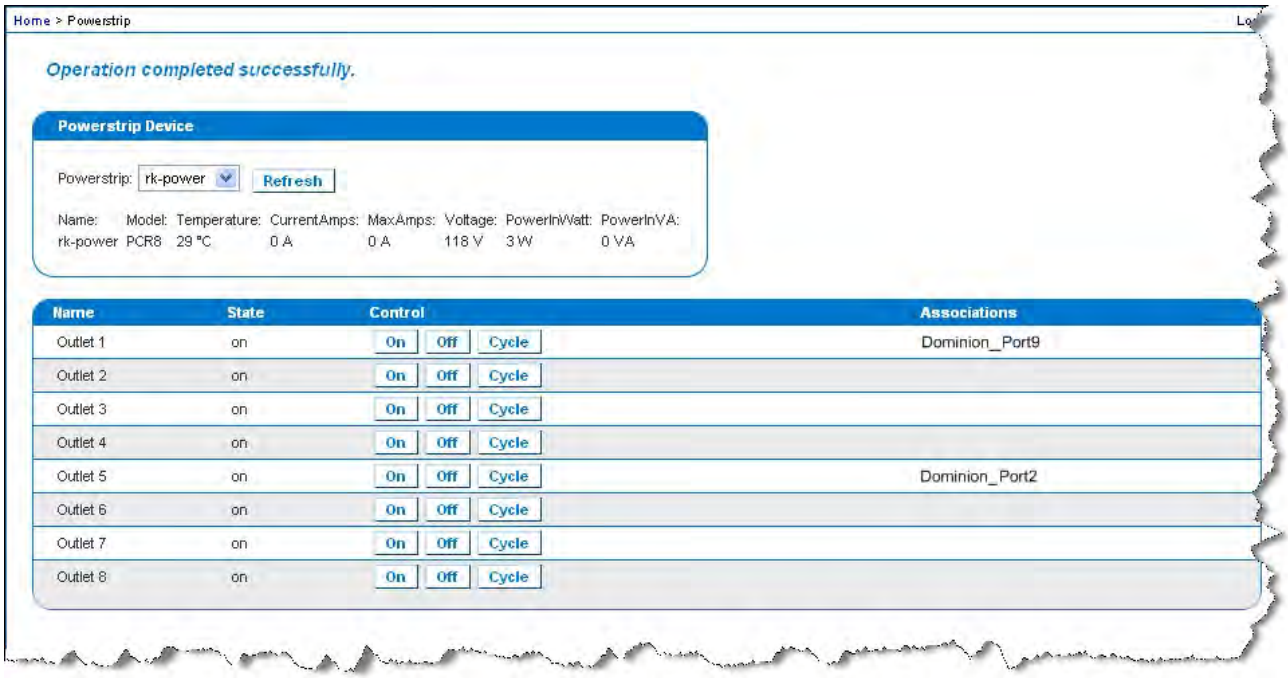
---

*Note: For information on setting up a PX, see the **Raritan PX User Guide**.*

From the Powerstrip page, you are able to turn the outlets on and off, as well as cycle their power. You are also able to view the following power strip and outlet information:

- Powerstrip Device Information:
  - Name
  - Model
  - Temperature
  - Current Amps
  - Maximum Amps
  - Voltage
  - Power in Watts
  - Power in Volts Ampere
- Outlet Display Information:
  - Name - Named assigned to the outlet when it was configured.
  - State - On or Off status of the outlet.
  - Control - Turn outlets on or off, or cycle their power.
  - Association - The ports associated with the outlet.

Initially, when you open the Powerstrip page, the power strips that are currently connected to the KSX II are displayed in the Powerstrip drop-down. Additionally, information relating to the currently selected power strip is displayed. If no power strips are connected to the KSX II, a message stating "No powerstrips found" will be displayed in the Powerstrip Device section of the page.


Home > Powerstrip
Operation completed successfully.
Powerstrip Device
Powerstrip: rk-power
Refresh
Name: Model: Temperature: CurrentAmps: MaxAmps: Voltage: PowerInWatt: PowerInVA:
rk-power PCR8 29 °C 0 A 0 A 118 V 3 W 0 VA
Name State Control Associations
Outlet 1 on On Off Cycle Dominion_Port9
Outlet 2 on On Off Cycle
Outlet 3 on On Off Cycle
Outlet 4 on On Off Cycle
Outlet 5 on On Off Cycle Dominion_Port2
Outlet 6 on On Off Cycle
Outlet 7 on On Off Cycle
Outlet 8 on On Off Cycle

Configuring KSX II Ports

The Port Configuration page displays a list of the KSX II ports. Ports connected to KVM target servers (blades and standard servers) and rack PDUs (power strips) are displayed in blue and can be edited. For ports with no CIM connected or with a blank CIM name, a default port name of Dominion_KSX2_Port# is assigned, where Port# is the number of the KSX II physical port.

To access a port configuration:

1. Choose Device Settings > Port Configuration. The Port Configuration Page opens.

   This page is initially displayed in port number order, but can be sorted on any of the fields by clicking on the column heading.

- Port Number - Numbered from 1 to the total number of ports available for the KSX II device.
- Port Name - The name assigned to the port.

Note: Do not use apostrophes for the Port (CIM) Name.

- Port Type:
  - DCIM - Dominion CIM
  - Not Available - No CIM connected
  - MCUTP - Master Console MCUTP, CIM in a cable
  - PCIM - Paragon CIM
  - PowerStrip (rack PDU) - Power strip connected
  - Dual - VM - Virtual media CIM (D2CIM-VUSB and D2CIM-DVUSB)
  - Blade Chassis - Blade chassis and the blades associated with that chassis (displayed in a hierarchical order)
  - KVM Switch - Generic KVM Switch connection
  - DVM-DP - Display Port
  - DVM-HDMI - HDMI CIM
  - DVM-DVI - DVI CIM

2. Click the Port Name for the port you want to edit.
   - For KVM ports, the Port page for KVM and blade chassis ports is opened.
   - For rack PDUs, the Port page for rack PDUs (power strips) is opened. From this page, you can name the rack PDUs and their outlets.
   - For serial ports, the Port page for serial ports is opened.

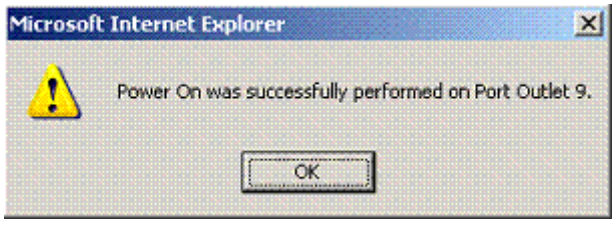
Port Configuration

No.	Name	Type
1	KX-local	Not Available
2	Dominion_KSX2_Port2	Not Available
3	KX8-Local	Not Available
4	Dominion_KSX2_Port4	Not Available
5	Blade_Chassis_Port3	Not Available
6	Dominion_KSX2_Port6	Not Available
7	Dominion_KSX2_Port7	Not Available
8	Dominion_KSX2_Port8	Not Available
9	Serial Port 1	Serial
10	Serial Port 2	Serial
11	Serial Port 3	Serial
12	Serial Port 4	Serial
13	Serial Port 5	Serial
14	Serial Port 6	Serial
15	Serial Port 7	Serial
16	Serial Port 8	Serial
17	Power Port 1	PowerStrip
18	Power Port 2	PowerStrip

Power Control

To turn an outlet on:

1. Click the Power menu to access the Powerstrip page.
2. From the Powerstrip drop-down, select the PX rack PDU (power strip) you want to turn on.
3. Click Refresh to view the power controls.
4. Click On.
5. Click OK to close the Power On confirmation dialog. The outlet will be turned on and its state will be displayed as 'on'.

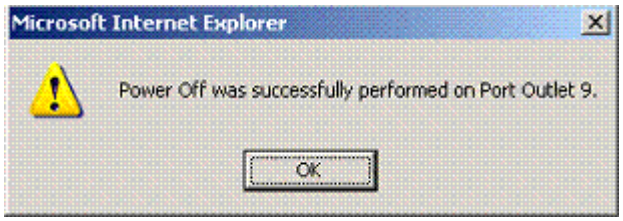


To turn an outlet off:

1. Click Off.

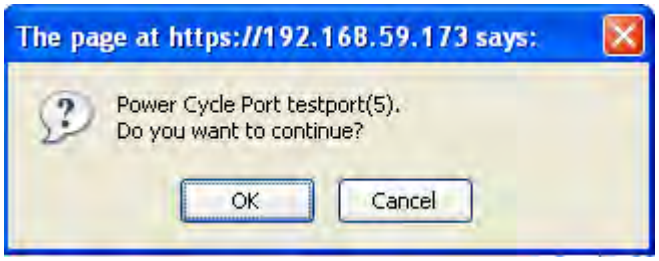
2. Click OK on the Power Off dialog.

3. Click OK on the Power Off confirmation dialog. The outlet will be turned off and its state will be displayed as 'off'.

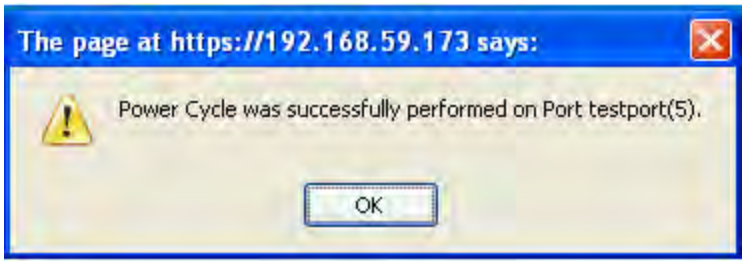


To cycle the power of an outlet:

1. Click Cycle. The Power Cycle Port dialog opens.



2. Click OK. The outlet will then cycle (note that this may take a few seconds).



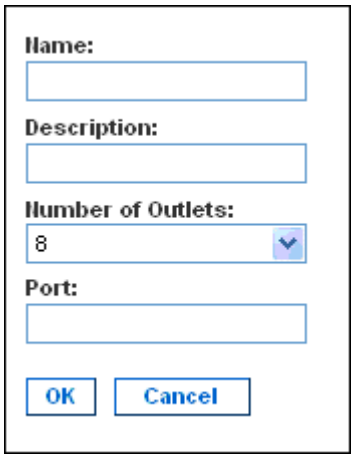
3. Once the cycling is complete the dialog will open. Click OK to close the dialog.

Dominion SX

By connecting to a Dominion SX device, you can associate one or more outlets on a PX device to specific Dominion SX ports.

Configuring a PX on Dominion SX

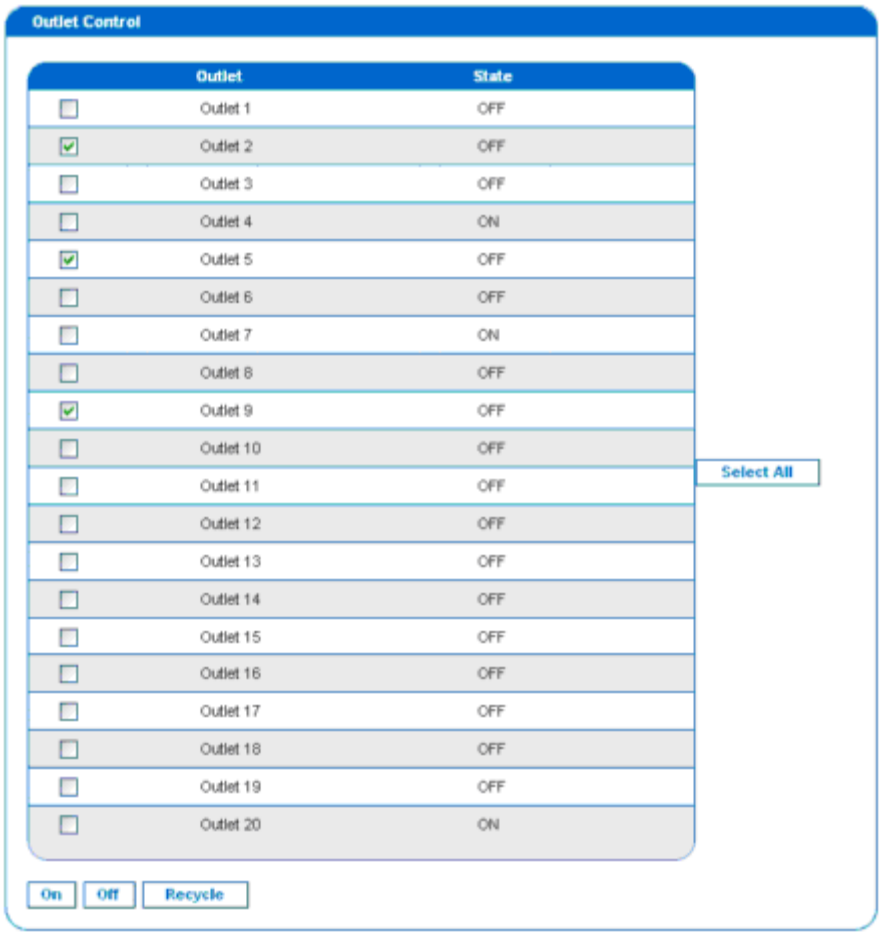
1. Choose Setup > Power Strip Configuration.
2. Click Add. The Power Strip Configuration screen appears.



3. Type a name and description in the Name and Description fields.
4. Select the number of outlets from the Number of Outlets drop-down menu.
5. Type the port number in the Port field.
6. Click OK.

Power Control

1. Choose Power Control > Power Strip Power Control. The Outlet Control screen appears.



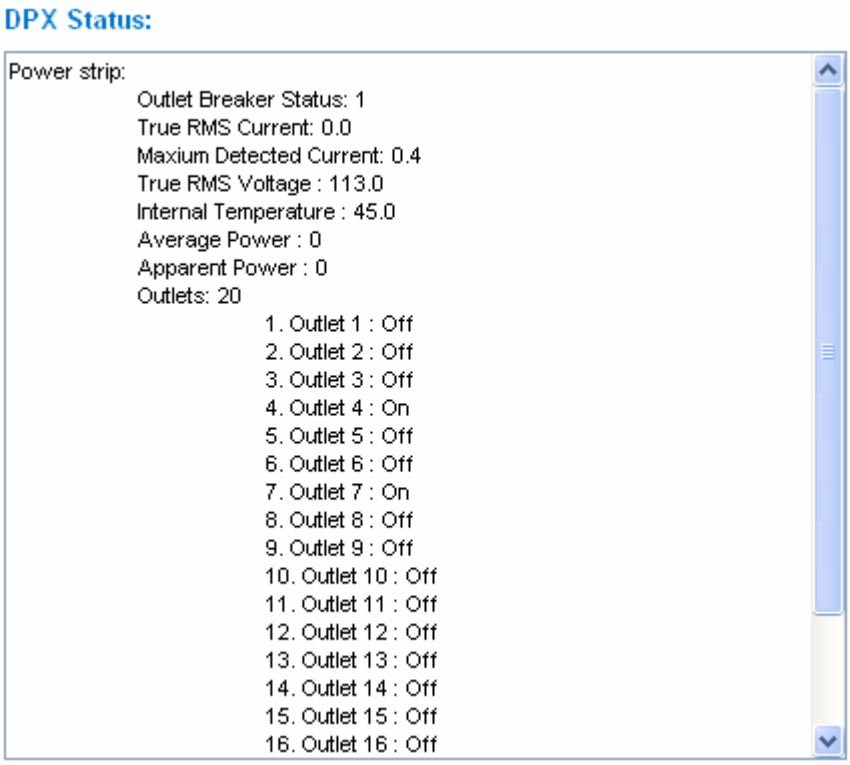
2. Check the box of outlet number you wish to control, and click On/Off buttons to power on/off the selected outlet(s).
3. A confirmation message appears, indicating successful operation.

Outlet 19: The power operation has been sent.

The system shall reflect successful operations shortly.

Checking Power Strip Status

1. Choose Power Control > Power Strip Status.


DPX Status:
Power strip:
Outlet Breaker Status: 1
True RMS Current: 0.0
Maxium Detected Current: 0.4
True RMS Voltage : 113.0
Internal Temperature : 45.0
Average Power : 0
Apparent Power : 0
Outlets: 20
1. Outlet 1 : Off
2. Outlet 2 : Off
3. Outlet 3 : Off
4. Outlet 4 : On
5. Outlet 5 : Off
6. Outlet 6 : Off
7. Outlet 7 : On
8. Outlet 8 : Off
9. Outlet 9 : Off
10. Outlet 10 : Off
11. Outlet 11 : Off
12. Outlet 12 : Off
13. Outlet 13 : Off
14. Outlet 14 : Off
15. Outlet 15 : Off
16. Outlet 16 : Off

2. A status box appears, displaying details of the controlled PX, including power state of each outlet on the device.

dcTrack

dcTrack® is a Raritan product that allows you to manage the data center. You can use dcTrack to:

- Record and manage the data center infrastructure and assets
- Monitor the electrical consumption of the data center
- Track environmental factors in the data center, such as temperature and humidity
- Optimize the data center growth

dcTrack Overview

dcTrack® is a powerful and intelligent data center management and automation application. dcTrack has been designed by data center and IT professionals to provide broad and deep visibility into the data center. It empowers data center managers to plan for growth and change by optimizing their current operations, assets, and infrastructure.

With dcTrack you can view everything in the data center from servers, blades, virtual servers and applications to data networks, IP addressing space and cabling. dcTrack also allows you to track real-time power consumption and manage raised floor space and rack elevations.

Use dcTrack to build your data center map directly or import existing data center information into the dcTrack. If you currently maintain data center information in spreadsheet format, that data can be imported into dcTrack using the Import wizard. Further, dcTrack allows you to import AutoCAD® objects to build a data center map.

Isolate potential problems with dcTrack since end-to-end power and data circuits can be visually and accurately traced while identifying all intermediate circuit points.

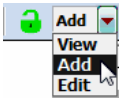
By using dcTrack's workflow and change management feature, data center managers are better able to enforce best practices across the enterprise and meet ITIL framework guidelines.

Adding the Raritan PX to dcTrack Management

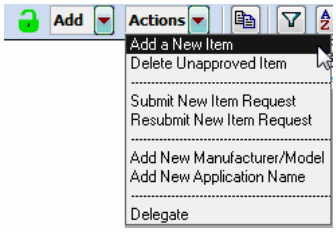
The Raritan PX is categorized as a rack PDU in dcTrack. This section describes the procedure to add the Raritan PX to dcTrack for management. For more information, see the dcTrack User Guide that accompanies the dcTrack.

To add a rack PDU:

1. From the Explorer Menu, select Power Items > Rack PDU.
2. Select Add from the Page Mode drop-down in the toolbar.



3. Select Add a New Item from the Actions drop-down in the toolbar.
4.



At a minimum, complete all of the required fields on the Detail 1 page. Complete additional fields as needed.

5. Enter the rack PDU ID.
6. Select the make and model.
7. Assign the rack PDU to cabinet and rail position.

Note: Once a status of Installed is applied to a item, placement fields cannot be edited in Edit mode. This means that rail positions cannot be changed once the item is installed. As a workaround, administrators can edit items from the Items & Ports page in Classic View.

8. Select the cabinet side if the rack PDU is vertically mounted.

Note: Twelve vertically mounted rack PDUs are supported per cabinet. Horizontally mounted/rack mounted rack PDUs do not apply to this step since there is no side to select.

9. If you are adding a Raritan PX2 device for asset sensor management purposes, see Adding a PX2 to Raritan PX for information on adding this item as a rack PDU.
10. Create ports as needed. See Creating Ports.
11. Complete all relevant Detail 2 information (if needed):
    a. Enter notes (if applicable).
    b. Enter maintenance and support information (if applicable).
    c. Complete custom user fields (if applicable).
12. Click Save. The saved item is given a status of Planned. Since the item has a status of new, it appears in red on the cabinet elevation.
13. To submit a request for approval, select Install Item Request from the Actions drop-down. After the Gatekeeper has reviewed and approved the request, a work order to physically add the item in the data center is generated by the Gatekeeper.

RF Code Energy Monitoring Solution

With the RF Code active RFID hardware and management software and Raritan's PX combined, a wire-free energy monitoring solution that provides a picture of power utilization is offered.

This combined solution does not require any additional IP address configuration or association. All you need to do is plug an RF Code R170 PDU sensor tag into the SENSOR port of the PX device.

The RF Code R170 PDU sensor tag collects the power data generated by Raritan PX and sends the data to the RF Code Sensor Manager software, which not only manages the power data but also make computations about the power usage from the collected data.

You can use the RF Code Sensor Manager to manage the power data using:

- Live table views
- Map views
- Interactive graphing and reporting
- Scheduled graphing and reporting
- Alerting and thresholding

Appendix F Additional PX Information

In This Chapter

MAC Address 496
Locking Outlets and Cords 496
Altitude Correction Factors 499
Data for BTU Calculation 499
Raritan Training Website 500
CLI Command Applicability 500
Truncated Data in the Web Interface 504
Reserving IP Addresses in Windows DHCP Servers 504

MAC Address

A label is affixed to a PX device, showing both the serial number and MAC address of the PDU.

If necessary, you can find the PDU's IP address through the MAC address by using commonly-used network tools. Contact your LAN administrator for assistance.

Locking Outlets and Cords

In addition to the cable retention clips, Raritan also provides other approaches to secure the connection of the power cords from your IT equipment to the Raritan PDUs, including:

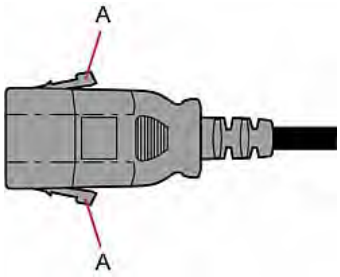
- SecureLock™ outlets and cords
- Button-type locking outlets

Note that NOT all Raritan PDUs are implemented with any of the above locking outlets.

SecureLock™ Outlets and Cords

SecureLock™ is an innovative mechanism designed by Raritan, which securely holds C14 or C20 plugs that are plugged into Raritan PDUs in place. This method requires the following two components:

- Raritan PDU with SecureLock™ outlets, which have a latch slot inside either side of the outlet.
- SecureLock™ cords, which is a power cord with a locking latch on either side of its plug. The following diagram illustrates such a plug.



Item	Description
A	Latches on the SecureLock™ cord's plug

Only specific PDUs are implemented with the SecureLock™ mechanism. If you PDU does not have this design, do NOT use the SecureLock™ cords with it.

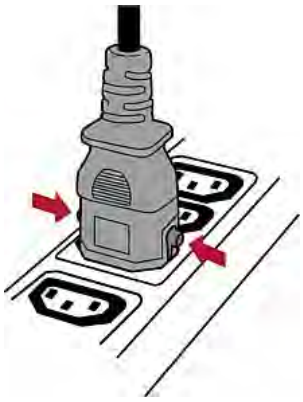
Tip: The SecureLock™ outlets can accept regular power cords for power distribution but the SecureLock™ mechanism does not take effect.

To lock a power cord using the SecureLock™ mechanism:

1. Verify that the SecureLock™ cord you purchased meets your needs.
   - The cords' female socket matches the power socket type (C14 or C20) on your IT equipment.
   - The cord's male plug matches the outlet type (C13 or C19) on your PDU.
2. Connect the SecureLock™ cord between the IT equipment and your PDU.
   - Plug the female socket end of the cord into the power socket of the desired IT equipment.
   - Plug the male plug end of the cord into the appropriate SecureLock™ outlet on the PDU. Push the plug toward the outlet until you hear the click, which indicates the plug's latches are snapped into the latch slots of the outlet.

To remove a SecureLock™ power cord from the PDU:

1. Press and hold down the two latches on the cord's plug as illustrated in the diagram below.



2. Unplug the cord now.

Button-Type Locking Outlets

A button-type locking outlet has a button on it. Such outlets do not require any special power cords to achieve the locking purpose. All you need to do is simply plug a regular power cord into the locking outlet and the outlet automatically locks the cord.

To remove a power cord from the locking outlet:

1. Press and hold down the tiny button on the outlet. Depending on the outlet type, the button location differs.

2. Unplug the power cord now.

Altitude Correction Factors

If a Raritan differential air pressure sensor is attached to your device, the altitude you enter for the device can serve as an altitude correction factor. That is, the reading of the differential air pressure sensor will be multiplied by the correction factor to get a correct reading.

This table shows the relationship between different altitudes and correction factors.

Altitude (meters)	Altitude (feet)	Correction factor
0	0	0.95
250	820	0.98
425	1394	1.00
500	1640	1.01
740	2428	1.04
1500	4921	1.15
2250	7382	1.26
3000	9842	1.38

Data for BTU Calculation

The heat generated by the PX device differs according to the model you purchased. To calculate the heat (BTU/hr), use the following power data according to your model type in the BTU calculation formula.

Model name	Maximum power (Watt)
PX2-1nnn series	5
PX2-2nnn series	20
PX2-3nnn series	24
PX2-4nnn series	24
PX2-5nnn series	24

The letter "n" included in the model names represents a number.

Raritan Training Website

Raritan offers free training materials for various Raritan products on the ***Raritan training website http://www.raritantraining.com***. The Raritan products introduced on this website include the intelligent PDU, dcTrack™, Power IQ, KVM and CommandCenter Secure Gateway (CC-SG). Raritan would update the training materials irregularly according to the latest development of Raritan products.

To get access to these training materials or courses, you need to apply for a username and password through the Raritan training website. After you are verified, you can access the Raritan training website anytime.

Having access to the training website could be helpful for learning or getting some ideas regarding Raritan products and making correct decisions on purchasing them. For example, you can take the dcTrack video training before implementing or using it.

CLI Command Applicability

Not every CLI command applies to all PX PDUs because features vary from model to model. For example, PX2-4nnn series (where n is a number) are not outlet-switching capable PDUs, so outlet-switching commands are NOT applicable.

The tables in this appendix show the command applicability for diverse PX product lines. In all tables:

- PX2-3k represents PX2-3000 series, ranging from PX2-3000 to PX2-3999
- PX2-4k represents PX2-4000 series, ranging from PX2-4000 to PX2-4999
- PX2-5k represents PX2-5000 series, ranging from PX2-5000 to PX2-5999

Show Commands

This table indicates the show commands applicability.

- Y: applicable
- N: NOT applicable

CLI commands	PX2-3k	PX2-4k	PX2-5k
`show assetStrip <n>`	Y	Y	Y
`show assetStripManagement`	Y	Y	Y
`show energywise`	Y	Y	Y
`show eventlog limit <n> class <event_type>`	Y	Y	Y

CLI commands	PX2-3k	PX2-4k	PX2-5k
show externalsensors <n> (details)	Y	Y	Y
show history	Y	Y	Y
show history bufferlength	Y	Y	Y
show inlets <n> (details)	N	Y	Y
show loadshedding	Y	Y	Y
show network (details)	Y	Y	Y
show network mode	Y	Y	Y
show network services <option>	Y	Y	Y
show network wireless (details)	Y	Y	Y
show ocp <n> (details)	Y	Y	Y
show outlets <n> (details)	Y (1)	Y (1)	Y
show pdu (details)	Y (2)	Y (2)	Y
show reliability data	Y	Y	Y
show reliability errorlog <n>	Y	Y	Y
show roles <role_name>	Y	Y	Y
show security (details)	Y	Y	Y
show sensor externalsensor <n> (details)	Y	Y	Y
show sensor inlet <n> <sensor type> (details)	N	Y	Y
show sensor inletpole <n> <p> <sensor type> (details)	N	Y	Y
show sensor ocp <n> <sensor type> (details)	Y	Y	Y
show sensor outlet <n> <sensor type> (details)	Y	Y	Y
show sensor outletpole <n> <p> <sensor type> (details)	Y	N	N
show serial	Y	Y	Y
show time (details)	Y	Y	Y
show user <user_name> (details)	Y	Y	Y
show user defaultPreferences	Y	Y	Y
show network wireless (details)	Y	Y	Y

Notes:

1. After performing the `show outlets <n>` command, the following outlet information is not available for PX2-3000 and PX2-4000 series:
   - State on device power up
   - Cycling power off period
2. After performing the `show pdu (details)` command, the following PDU information is not available for PX2-3000 and PX2-4000 series:
   - Default outlet state on startup
   - Outlet power sequence
   - Outlet power sequence delay

Configuration Commands

This table indicates the configuration commands applicability.

- Y: applicable
- N: NOT applicable

CLI commands	PX2-3k	PX2-4k	PX2-5k
All `network` commands	Y	Y	Y
All `security` commands	Y	Y	Y
All `inlet` commands	Y	Y	Y
All `ocp` commands	Y	Y	Y
All `externalsensor` commands	Y	Y	Y
All `sensor outlet` commands	Y	Y	Y
All `sensor inlet` commands	Y	Y	Y
All `sensor inletpole` commands	Y	Y	Y
All `sensor ocp` commands	Y	Y	Y
All `sensor externalsensor` commands	Y	Y	Y
All `serial` commands	Y	Y	Y
All `time` commands	Y	Y	Y
All `user` commands	Y	Y	Y
All `role` commands	Y	Y	Y
All `energywise` commands	Y	Y	Y
All `assetStrip` commands	Y	Y	Y

CLI commands	PX2-3k	PX2-4k	PX2-5k
All `loadshedding` commands	N	N	Y
`history length <n>`	Y	Y	Y
`network mode <mode>`	Y	Y	Y
`outlet <n> cyclingPowerOffPeriod <timing>`	N	N	Y
`outlet <n> name "<name>"`	Y	Y	Y
`outlet <n> stateOnDeviceStartup <option>`	N	N	Y
`pdu cyclingPowerOffPeriod <timing>`	Y	Y	Y
`pdu dataRetrieval <option>`	Y	Y	Y
`pdu deviceAltitude <altitude>`	Y	Y	Y
`pdu externalSensorsZCoordinateFormat <option>`	Y	Y	Y
`pdu inrushGuardDelay <timing>`	N	N	Y
`pdu measurementsPerLogEntry <number>`	Y	Y	Y
`pdu name "<name>"`	Y	Y	Y
`pdu nonCriticalOutlets <outlets1>:false;<outlets2>:true`	N	N	Y
`pdu displayOrientation <orientation>`	Y (1)	Y (1)	Y (1)
`pdu outletInitializationDelayOnDeviceStartup <timing>`	N	N	Y
`pdu outletSequence <option>`	N	N	Y
`pdu outletSequenceDelay <outlet1>:<delay1>;<outlet2>:<delay2>; <outlet3>:<delay3>;...`	N	N	Y
`pdu outletStateOnDeviceStartup <option>`	N	N	Y

Notes:

1. The `pdu displayOrientation <orientation>` command only applies to Zero U models.

Other Commands

This table indicates the applicability of CLI commands other than the show and configuration commands.

- Y: applicable
- N: NOT applicable

CLI commands	PX2-3k	PX2-4k	PX2-5k
`clear eventlog`	Y	Y	Y
`factorydefaults`	Y	Y	Y
All `power outlets` commands	N	N	Y
All `reset pdu` commands	Y	Y	Y
`nslookup <host>`	Y	Y	Y
`netstat <option>`	Y	Y	Y
`ping <host>`	Y	Y	Y
`traceroute <host>`	Y	Y	Y

Truncated Data in the Web Interface

Some fields of the PX web interface can accommodate data entry up to 256 characters. When the data entered is too long, it may be truncated due to some or all of the following factors:

- Screen resolution
- Font size
- Font type
- Size of different characters

Current web browser technology cannot break or wrap these fields with long inputs.

The solution for this issue includes:

- Increase of the screen resolution
- Application of smaller font size
- Use of other interfaces, such as the CLI or SNMP, to view the data in these fields

Reserving IP Addresses in Windows DHCP Servers

The PX uses its serial number as the client identifier in the DHCP request. Therefore, to successfully reserve an IP address for the PX in a Windows® DHCP server, use the PX device's serial number as the unique ID instead of the MAC address.

Convert the serial number into ASCII codes for the IP address reservation entry. For example, if the PX device's serial number is PEG1A0003, use the serial number's ASCII codes "50 45 47 31 41 30 30 30 30 33" as the unique ID.

Index

1

1U Products • 4

2

2U Products • 4

A

A Note about Enabling Thresholds • 272
A Note about Firmware Upgrade Time • 259
A Note about Infinite Loop • 211
A Note about Untriggered Rules • 215
About the Interface • 273
Access Security Control • 128
Accessing the Help • 261
Action Group • 181, 183
Activating or Deactivating the Load Shedding Mode • 169
Add Page Icon • 83, 87
Adding a Firewall Rule • 345
Adding a Role-Based Access Control Rule • 362
Adding Authentication Servers • 149
Adding IT Devices for Ping Monitoring • 217
Adding PDUs to Power IQ Management • 478
Adding the LDAP Server Settings • 149
Adding the RADIUS Server Settings • 152
Adding the Raritan PX to dcTrack Management • 493
Additional PX Information • 496
Adjusting Snapshot or Video Properties • 243
Adjusting the Pane • 85
Alert States and LHX Event Log • 256
Alerted Sensors • 93
All Privileges • 418, 421, 422
Altitude Correction Factors • 115, 312, 499
AMS-M2-Z Daisy-Chain Limitations • 54, 55, 56
Applicable Models • xiv
Asset Management • 232
Asset Management Commands • 425
Asset Sensor Management • 426
Asset Sensor Settings • 297
Associating Outlets with Target Servers on KX II and LX • 483
Automatic Mode • 68, 456
Automatically Completing a Command • 446

B

Backup and Restore of PX Device Settings • xvi, 238, 240
Beeper • 76
Before You Begin • 13
Blade Extension Strip Settings • 299
Browser-Defined Shortcut Menu • 92
Browsing through the Online Help • 261
Built-in Wireless LAN Adapters • xvi, 21
Bulk Configuration • 238, 241
Bulk Configuration for Circuit Breaker Thresholds • 177
Bulk Configuration for Outlet Thresholds • 174
Button-Type Locking Outlets • 498

C

Cascading the PX via USB • xvi, 29, 64, 95
Certificate Signing Request • 143
Change Load Shedding State • 182, 190
Changing a User's Password • 406
Changing an Outlet's Default State • 367
Changing the Circuit Breaker Name • 369
Changing the Column • 91
Changing the Cycling Power-Off Period • 161
Changing the Default Policy • 129, 138, 139
Changing the HTTP Port • 332
Changing the HTTP(S) Settings • 105
Changing the HTTPS Port • 332
Changing the Inlet Name • 369
Changing the LAN Duplex Mode • 331
Changing the LAN Interface Speed • 330
Changing the LED Display Orientation • 66, 313
Changing the Measurement Units • 413, 416
Changing the Modbus Configuration • 337
Changing the Modbus Port • 339
Changing the Modbus/TCP Settings • 108
Changing the Outlet Name • 366
Changing the Outlet-Specific Cycling Power-Off Period • 162, 163
Changing the PDU Name • 306
Changing the PDU-Defined Cycling Power-Off Period • 162, 163
Changing the Role List View • 128
Changing the Role(s) • 412
Changing the Sensor Description • 374

Changing the Sensor Name • 370
Changing the Sorting • 91, 217, 221
Changing the SSH Configuration • 333
Changing the SSH Port • 334
Changing the SSH Settings • 106, 122
Changing the Telnet Configuration • 332
Changing the Telnet Port • 333
Changing the Telnet Settings • 106
Changing the UDP Port • 425
Changing the User List View • 124
Changing the View of a List • 90, 124, 128, 247
Changing Your Own Password • 415
Changing Your Password • 80
Checking Power Strip Status • 492
Checking Server Monitoring States • 221
Checking the Branch Circuit Rating • xvi, 14
Circuit Breaker Configuration Commands • 369
Circuit Breaker Information • 284
Circuit Breaker Orientation Limitation • 5, 6, 7, 9, 10, 11
Circuit Breaker Sensor Threshold Information • 291
Circuit Breakers • 71
Clearing Event Entries • 216
Clearing Event Log • 304
Clearing Information • 304
CLI Command Applicability • 500
Closing a Local Connection • 276
Collapsing the Tree • 85
Combining Asset Sensors • 47
Command History • 301
Commands for Circuit Breaker Sensors • 394
Commands for Environmental Sensors • 399
Commands for Inlet Pole Sensors • 386
Commands for Inlet Sensors • 380
Commands for Outlet Sensors • 374
Components of an Event Rule • 180
Configuration Commands • 502
Configuring a Contact Closure Sensor • 41, 43, 230, 231
Configuring a PX on Dominion SX • 490
Configuring a Specific Rack Unit • 234, 235
Configuring Environmental Sensors • 222, 224, 227
Configuring IP Protocol Settings • 315
Configuring KSX II Ports • 486
Configuring NTP Server Settings • xvi, 272
Configuring Rack PDU (Power Strip) Targets • 480
Configuring SNMP Notifications • 208, 209, 220, 265
Configuring Temperature and Fan Thresholds • 253
Configuring the Asset Sensor • 50, 233
Configuring the Feature Port • 113, 252
Configuring the Firewall • 128
Configuring the IPv4 Parameters • 322
Configuring the IPv6 Parameters • 326
Configuring the LHX Device • 251, 252
Configuring the PX • 16, 101
Configuring the PX Device and Network • 305
Configuring the Serial Port • 114
Configuring the SMTP Settings • 117, 185, 186
Configuring the SNMP Settings • 107, 121
Configuring Users for Encrypted SNMP v3 • 107, 264
Configuring Webcam Storage • 245, 247
Configuring Webcams • 242, 243, 247
Connecting a GSM Modem (Optional) • 59
Connecting a Logitech Webcam (Optional) • xvi, 58, 83, 242, 243
Connecting a Rack PDU • 480
Connecting a Schroff LHX Heat Exchanger (Optional) • 59, 113, 251
Connecting AMS-M2-Z Asset Sensors (Optional) • 54, 57
Connecting an RF Code PDU Sensor Tag (Optional) • 60
Connecting Asset Sensors to the PX • 49, 54
Connecting Blade Extension Strips • 51
Connecting Detectors/Switches to DPX-CC2-TR • 36, 37
Connecting Detectors/Switches to New DPX-CC2-TR • xvi, 36, 38
Connecting Environmental Sensors (Optional) • 33, 58, 221
Connecting External Equipment • 33
Connecting the Asset Management Sensor (Optional) • 47, 64, 113, 232
Connecting the PDU to a Power Source • 15
Connecting the PX to a Computer • 17, 467, 468
Connecting the PX to Your Network • 20, 99, 100
Connection Ports • 63
Contact Closure Sensor LEDs • xvi, 43
Contact Closure Sensors • 35
Copying a PX Configuration • 240
Correctly Displaying the LHX Device • 252
Creating a Certificate Signing Request • 143
Creating a Role • 122, 125, 417
Creating a Self-Signed Certificate • 145

Creating a User Profile • 78, 106, 120, 123, 124, 125, 126, 264, 404
Creating Actions • xvi, 59, 181, 213, 242
Creating an Event Rule • 180
Creating Firewall Rules • 129, 130
Creating Role-Based Access Control Rules • 138, 139
Creating Rules • 194

D

Dashboard Page • 458
Data for BTU Calculation • 499
Data Pane • 88
Date and Time Settings • 284
dcTrack • xvii, 492
dcTrack Overview • 493
Default Log Messages • 137, 186, 198
Default Measurement Units • 285
Deleting a Firewall Rule • 349
Deleting a Role • 127, 422
Deleting a Role-Based Access Control Rule • 366
Deleting a User Profile • 124, 414
Deleting an Event Rule or Action • 214
Deleting Firewall Rules • 133
Deleting Ping Monitoring Settings • 220
Deleting Role-Based Access Control Rules • 142
Deleting the Authentication Server Settings • 154
Derating a Raritan Product • 450
Describing the Sensor Location • 225, 227
Determining the Time Setup Method • 340
Device Management • 94
Device States and Icon Variations • 252, 255, 257
Diagnostic Commands • 443
Different CLI Modes and Prompts • 275, 276, 279, 304, 305, 437, 438
Differential Air Pressure Sensors • 46
Disabling External Authentication • 154
Displaying the Asset Sensor Information • 237
Displaying the PDU Information • 94
Dominion KSX II • 484
Dominion KSX II or SX Configuration • xvii, 113, 484
Dominion KX II Configuration • 113, 480
Dominion PX Explorer Pane • 82
Dominion SX • 489
Downloading Diagnostic Information • 250
Downloading Key and Certificate Files • 147
Downloading SNMP MIB • 108, 264, 265, 266, 268, 270

E

Editing Firewall Rules • 132
Editing Ping Monitoring Settings • 220
Editing Role-Based Access Control Rules • 141
Editing the Authentication Server Settings • 153
Email and SMS Message Placeholders • 186, 187, 191, 206
Enabling and Disabling Schroff LHX Heat Exchanger Support • 184, 192, 251, 252
Enabling and Editing the Security Banner • xvi, 137
Enabling Data Logging • 116
Enabling External and Local Authentication Services • 155
Enabling IPv4 or IPv6 • 315
Enabling Login Limitations • 135
Enabling or Disabling a User Profile • 408
Enabling or Disabling Data Logging • 311
Enabling or Disabling EnergyWise • 423
Enabling or Disabling Load Shedding • 437
Enabling or Disabling Modbus • 338
Enabling or Disabling SNMP v1/v2c • 335
Enabling or Disabling SNMP v3 • 335
Enabling or Disabling SSH • 334
Enabling or Disabling Strong Passwords • 356
Enabling or Disabling Telnet • 333
Enabling or Disabling the Read-Only Mode • 338
Enabling or Disabling the Restricted Service Agreement • 350
Enabling or Disabling the Service Advertisement • 339
Enabling Password Aging • 136
Enabling Service Advertisement • 109, 339
Enabling SNMP • 116, 263
Enabling Strong Passwords • 135
Enabling the Feature • 138
Enabling the Firewall • 128, 129
Enabling User Blocking • 134
EnergyWise Configuration Commands • 423
EnergyWise Settings • 297
Entering the Configuration Mode • 276, 305, 320, 406, 415
Entering the Diagnostic Mode • 276, 443
Environmental Sensor Configuration Commands • 370
Environmental Sensor Information • 286

Environmental Sensor Threshold Information • 293
Environmental Sensors • 221
Equipment Setup Worksheet • 14, 463
Event Log • 300
Event Rules and Actions • 107, 117, 173, 180, 217, 265
Example • 306, 307, 308, 309, 310, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 322, 323, 324, 325, 326, 327, 328, 329, 330, 331, 332, 333, 334, 335, 336, 337, 338, 339, 340, 341, 342, 343, 345, 347, 349, 350, 351, 352, 353, 354, 355, 356, 357, 358, 359, 361, 363, 365, 366, 367, 368, 369, 370, 371, 372, 373, 374, 375, 376, 377, 378, 379, 380, 381, 382, 383, 384, 385, 386, 388, 389, 390, 391, 392, 394, 395, 396, 397, 398, 399, 400, 401, 402, 403, 404, 405, 406, 407, 408, 412, 414, 415, 417, 420, 422, 423, 424, 425, 426, 427, 428, 429, 430, 431, 432, 433, 434, 437, 439, 440, 441, 443, 444, 445, 446
  Ping Monitoring and SNMP Notifications • 219
  When Hysteresis is Useful • 179
  When to Disable Hysteresis • 179
Example 1 • 212
Example 1 - Basic Security Information • 302
Example 1 - Combination of IP, Subnet Mask and Gateway Parameters • 435
Example 2 • 212
Example 2 - Combination of Upper Critical and Upper Warning Settings • 435
Example 2 - In-Depth Security Information • 303
Example 3 • 212
Example 3 - Basic PDU Information • 303
Example 3 - Combination of SSID and PSK Parameters • 436
Example 4 - Combination of Upper Critical, Upper Warning and Lower Warning Settings • 436
Example 4 - In-Depth PDU Information • 304
Examples • 302
Existing Roles • 296
Existing User Profiles • 285, 295
Expanding a Blade Extension Strip • 236
Expanding the Tree • 83, 155, 156, 157, 158, 159, 161, 163, 168, 169, 170, 171, 172, 173, 174, 175, 176, 177, 222, 223, 224, 228, 232, 254

F

Feature RJ-45 Port Pinouts • 461
Filling Out the Equipment Setup Worksheet • 14
Firewall Control • 343
Firmware Upgrade • 240, 258
Flexible Cord Installation Instructions • 449
Flexible Cord Selection • 449
Floor Water Sensors • xvi, 43
Forcing a Password Change • 408
Forcing HTTPS Encryption • 105, 128, 142
Full Disaster Recovery • 260
Fuse • 73
Fuse Replacement on 1U Models • 74
Fuse Replacement on Zero U Models • 73

G

Gathering the External Authentication Information • 148
Gathering the LDAP Information • 148
Gathering the RADIUS Information • 149

H

Help Command • 277
History Buffer Length • 301
How to Use the Calendar • 111
HTTPS Access • 352

I

Identifying Environmental Sensors • 221, 222, 223
Identifying the Cascaded Devices • xvi, 30, 94, 95
Idle Timeout • 354
Initial Network Configuration • 22, 78, 86, 99, 100, 467, 468, 469
Inlet and Circuit Breaker Management • 170
Inlet Configuration Commands • 368
Inlet Information • 283
Inlet Pole Sensor Threshold Information • 290
Inlet Sensor Threshold Information • 289
In-Line Monitor Unused Channels • 451
In-Line Monitors • 448
In-Line Monitor's LED Display • 456
In-Line Monitor's Web Interface • 457
Installation and Configuration • 13
Installing a CA-Signed Certificate • 144

Installing Cable Retention Clips on Outlets (Optional) • 31
Installing Cable Retention Clips on the Inlet (Optional) • 14
Installing Existing Key and Certificate Files • 146
Installing the USB-to-Serial Driver (Optional) • xvi, 18, 270
Integration • 478
Introduction • 1
Introduction to the Web Interface • 81
IP Configuration • 279

L

LAN Interface Settings • 280
Layout • 271
LDAP Configuration Illustration • 151, 470
LED Display • 65, 456
LEDs for Measurement Units • 67, 69, 457
Listing TCP Connections • 249
Load Shedding Configuration Commands • 437
Load Shedding Settings • 296
Locking Outlets and Cords • 32, 496
Log an Event Message • 181, 184
Logging in to CLI • 274
Logging in to the Web Interface • 78
Logging out of CLI • 447
Login • 78
Login Limitation • 352
Logout • 80
Logout Button • 88
Lowercase Character Requirement • 357

M

MAC Address • 16, 496
Managing Environmental Sensors • 221, 223
Managing Event Logging • 215
Managing Firewall Rules • 345
Managing Role-Based Access Control Rules • 361
Managing the Schroff LHX Heat Exchanger • xvi, 59, 113, 251
Managing the Snapshots Saved to PX • 246
Manual Mode • 69, 71, 456
Marking All Outlets • 167
Marking an Outlet • 168
Maximum Ambient Operating Temperature • 14, 460
Maximum Password History • 359
Maximum Password Length • 357
Menus • 82
Minimum Password Length • 356
Modifying a Firewall Rule • 347
Modifying a Role • 122, 123, 126, 420
Modifying a Role-Based Access Control Rule • 363
Modifying a User Profile • 80, 123, 126, 405
Modifying a User's Personal Data • 407
Modifying an Action • 108, 214
Modifying an Event Rule • 213
Modifying the Firewall Control Parameters • 344
Modifying the IPv4 Settings • 102
Modifying the IPv6 Settings • 103
Modifying the Network Configuration • 98
Modifying the Network Interface Settings • 99
Modifying the Network Service Settings • 105, 273, 275
Modifying the Network Settings • 86, 101, 109, 472
Modifying the Role-Based Access Control Parameters • 360
Modifying the SNMPv3 Settings • 409
Monitoring All Outlets • 156
Monitoring an Outlet • 157
Monitoring Circuit Breakers • 172
Monitoring Server Accessibility • 217
Monitoring the Inlet • 171
Monitoring the LHX Device • 251, 254
More Information • 88
More Information about AD Configuration • 151
Mounting 1U or 2U Models • 11
Mounting Zero U Models Using Button Mount • 7
Mounting Zero U Models Using Claw-Foot Brackets • 9
Mounting Zero U Models Using L-Brackets • 6
Mounting Zero U Models Using Two Rear Buttons • 10
Multi-Command Syntax • 345, 352, 355, 361, 405, 407, 409, 413, 416, 435

N

Naming a Rack Unit • 430
Naming an Asset Sensor • 426
Naming Circuit Breakers • 170
Naming Outlets • 155
Naming the Inlet • 170

Naming the PDU • 83, 85, 86, 98, 115, 158, 159, 160, 162, 164, 165, 166, 167, 169, 170, 171, 174, 175, 176, 177, 222, 223, 224, 226, 228, 232, 254
Naming the Rack PDU in the KX II or LX (Port Page for Power Strips) • 481
Network Configuration • 279
Network Diagnostics • 248
Network Service Settings • 281
Network Troubleshooting • 248, 442
Networking Configuration Commands • 314
Networking Mode • 280
Numeric Character Requirement • 358

O

Old and New Contact Closure Sensors • 36
Operating Hours • 256
Other Commands • 503
Outlet Configuration Commands • 366
Outlet Information • 282
Outlet Management • 155
Outlet Monitoring • 156
Outlet Page • 458
Outlet Pole Sensor Threshold Information • 288
Outlet Sensor Threshold Information • 287
Outlet Switching • 158
Outlets • 61
Overriding the DHCP-Assigned NTP Servers • 341
Overriding the IPv4 DHCP-Assigned DNS Server • 326
Overriding the IPv6 DHCP-Assigned DNS Server • 329, 330
Overview • 448, 485

P

Package Contents • 4, 13
Panel Components • 61
Password Aging • 353
Password Aging Interval • 354
PDU Configuration • 281
PDU Configuration Commands • 305
Pinging a Host • 248
Plug Selection • 450
Power Control • 488, 491
Power Control Operations • 438
Power Cord • 61
Power Cycling the Outlet(s) • 440
Power IQ Configuration • 478
Power Measurement Accuracy • 460
Preparing the Installation Site • 13
Product Features • xv, 1
Product Models • 1
Providing the EAP CA Certificate • 319
PX2-3000 Series • 62
PX2-4000 Series • 62
PX2-5000 Series • 62

Q

Querying Available Parameters for a Command • 277, 278
Querying the DNS Servers • 443
Quitting the Configuration Mode • 305, 351, 436
Quitting the Diagnostic Mode • 446

R

Rack Unit Configuration • 430
Rack Unit Settings of an Asset Sensor • 298
Rackmount Safety Guidelines • 5
Rack-Mounting the PDU • 5
Raritan Training Website • xvii, 500
Rebooting the PX Device • 119
Receptacle Selection • 450
Record Snapshots to Webcam Storage • 182, 193
Reliability Data • 302
Reliability Error Log • 302
Request LHX Maximum Cooling • 181, 184
Requesting Maximum Cooling for an LHX • 256, 257
Reserving IP Addresses in Windows DHCP Servers • xvii, 504
Reset Button • 70
Resetting the Button-Type Circuit Breaker • 71
Resetting the Handle-Type Circuit Breaker • 72
Resetting the PX • 442
Resetting to Factory Defaults • 70, 442, 467
Resizing a Dialog • 92
Restarting the PDU • 442
Restricted Service Agreement • 350
Retrieving Energy Usage • 272
Retrieving Previous Commands • 446
Retrieving Software Packages Information • 261
RF Code Energy Monitoring Solution • 60, 495
Role Configuration Commands • 417
Role of a DNS Server • 105, 472

Role-Based Access Control • 360

S

Safety Guidelines • ii
Safety Instructions • iii, 14, 448
Sample Environmental-Sensor-Level Event Rule • 210
Sample Event Rules • 208
Sample Inlet-Level Event Rule • 209
Sample Outlet-Level Event Rule • 208
Sample PDU-Level Event Rule • 208
Saving a PX Configuration • 239
Saving Snapshots • 242, 244, 246
SecureLock™ Outlets and Cords • 497
Security Configuration Commands • 343
Security Settings • 294
Selecting IPv4 or IPv6 Addresses • 315
Selecting the Internet Protocol • 102, 103
Send a Snapshot via Email • 181, 184
Send an SNMP Notification • 182, 187
Send EMail • 181, 186, 198
Send SMS Message • 182, 191
Sending Snapshots or Videos in an Email or Instant Message • 242, 244
Sensor Measurement Accuracy • xvi, 229
Sensor RJ-12 Port Pinouts • 461
Sensor Threshold Configuration Commands • 374
Serial Port Configuration Commands • 433
Serial Port Settings • 297
Serial RS-232 Port Pinouts • 461
Setting a Circuit Breaker's Thresholds • 176, 177
Setting an LED Color for a Rack Unit • 431, 432
Setting an LED Mode for a Rack Unit • 431, 433
Setting an Outlet's Cycling Power-Off Period • 368
Setting an Outlet's Thresholds • 173, 174
Setting Asset Sensor LED Colors • 234
Setting Data Logging • 116, 311
Setting Default Measurement Units • 413, 416
Setting Inlet Thresholds • 175
Setting LED Colors for Connected Tags • 429, 431, 432
Setting LED Colors for Disconnected Tags • 429, 431, 432
Setting Non-Critical Outlets and Load Shedding Mode • 167, 190, 310
Setting Power Thresholds • 90, 173, 271
Setting the Authentication Method • 317
Setting the Automatic Daylight Savings Time • 342
Setting the BSSID • 322
Setting the Circuit Breaker's Assertion Timeout • 398
Setting the Circuit Breaker's Deassertion Hysteresis • 398
Setting the Data Logging Measurements Per Entry • 311
Setting the Date and Time • 110, 272
Setting the Default Outlet State • 160
Setting the EAP Identity • 319
Setting the EAP Parameters • 318
Setting the EAP Password • 319
Setting the EnergyWise Configuration • 118
Setting the History Buffer Length • 434
Setting the Initialization Delay • 164, 310
Setting the Inlet Pole's Assertion Timeout • 393
Setting the Inlet Pole's Deassertion Hysteresis • 391
Setting the Inlet's Assertion Timeout • 386
Setting the Inlet's Deassertion Hysteresis • 385
Setting the Inlet's Lower Critical Threshold • 383
Setting the Inlet's Lower Warning Threshold • 384
Setting the Inlet's Upper Critical Threshold • 381
Setting the Inlet's Upper Warning Threshold • 382
Setting the Inner Authentication • 318
Setting the Inrush Guard Delay • 165
Setting the Inrush Guard Delay Time • 309
Setting the IPv4 Address • 323
Setting the IPv4 Configuration Mode • 322
Setting the IPv4 Gateway • 324
Setting the IPv4 Preferred Host Name • 323
Setting the IPv4 Primary DNS Server • 325
Setting the IPv4 Secondary DNS Server • 325
Setting the IPv4 Subnet Mask • 324
Setting the IPv6 Address • 328
Setting the IPv6 Configuration Mode • 326
Setting the IPv6 Gateway • 328
Setting the IPv6 Preferred Host Name • 327
Setting the IPv6 Primary DNS Server • 329
Setting the IPv6 Secondary DNS Server • 329
Setting the LAN Interface Parameters • 330
Setting the LED Operation Mode • 431
Setting the Lower Critical Threshold for a Circuit Breaker • 396
Setting the Lower Critical Threshold for an Inlet Pole • 389

Setting the Lower Warning Threshold for a Circuit Breaker • 397
Setting the Lower Warning Threshold for an Inlet Pole • 390
Setting the Network Service Parameters • 331
Setting the Networking Mode • 314
Setting the NTP Parameters • 340
Setting the Outer Authentication • 318
Setting the Outlet Initialization Delay • 310
Setting the Outlet Power-On Sequence • 165, 306
Setting the Outlet Power-On Sequence Delay • 307
Setting the Outlet's Assertion Timeout • 380
Setting the Outlet's Deassertion Hysteresis • 379
Setting the Outlet's Lower Critical Threshold • 377
Setting the Outlet's Lower Warning Threshold • 378
Setting the Outlet's Upper Critical Threshold • 374
Setting the Outlet's Upper Warning Threshold • 376
Setting the Outlet-Specific Default State • 160, 161
Setting the Outlet-Specific Power-On Delay • 166
Setting the PDU-Defined Cycling Power-Off Period • 309, 368
Setting the PDU-Defined Default Outlet State • 308, 367
Setting the PDU-Defined Default State • 160, 161
Setting the Polling Interval • 425
Setting the PSK • 317
Setting the Sensor's Assertion Timeout • 403
Setting the Sensor's Deassertion Hysteresis • 403
Setting the Sensor's Lower Critical Threshold • 401
Setting the Sensor's Lower Warning Threshold • 402
Setting the Sensor's Upper Critical Threshold • 399
Setting the Sensor's Upper Warning Threshold • 400
Setting the Serial Port Baud Rate • 434
Setting the SNMP Configuration • 334
Setting the SNMP Read Community • 336
Setting the SNMP Write Community • 336
Setting the SSID • 316
Setting the sysContact Value • 336
Setting the sysLocation Value • 337
Setting the sysName Value • 337
Setting the Time Zone • 272, 342
Setting the Upper Critical Threshold for a Circuit Breaker • 394
Setting the Upper Critical Threshold for an Inlet Pole • 387
Setting the Upper Warning Threshold for a Circuit Breaker • 395
Setting the Upper Warning Threshold for an Inlet Pole • 388
Setting the Wireless Parameters • 316
Setting the X Coordinate • 372
Setting the Y Coordinate • 372
Setting the Z Coordinate • 313, 373
Setting the Z Coordinate Format • 226
Setting the Z Coordinate Format for Environmental Sensors • 312, 373
Setting Thresholds for Multiple Sensors • xvi, 227
Setting Up an LHX • 253
Setting Up an SSL Certificate • 128, 142
Setting Up Default Measurement Units • xvi, 112, 124
Setting Up External Authentication • xvi, 105, 128, 147
Setting Up Role-Based Access Control Rules • 138
Setting Up Roles • 80, 116, 119, 122, 125
Setting Up User Login Controls • 134
Setting Up Your Preferred Measurement Units • xvi, 112, 115, 123, 124
Setup Button • 85
Show Commands • 500
Showing Information • 279
Showing the Network Connections • 444
Single Login Limitation • 353
Snapshot Storage • xvi, 245
SNMP Gets and Sets • 269
SNMP Sets and Thresholds • 271
SNMPv2c Notifications • 266
SNMPv3 Notifications • 267
Sorting Firewall Rules • 133
Sorting Role-Based Access Control Rules • 141
Sorting the Access Order • 153
Special Character Requirement • 358
Specifications • 5, 460
Specifying Non-Critical Outlets • 296, 310

Specifying the Agreement Content • 351
Specifying the Asset Sensor Orientation • 428
Specifying the Device Altitude • 115, 312
Specifying the EnergyWise Domain • 424
Specifying the EnergyWise Secret • 424
Specifying the Number of Rack Units • 426
Specifying the Primary NTP Server • 340
Specifying the Rack Unit Numbering Mode • 427
Specifying the Rack Unit Numbering Offset • 428
Specifying the Secondary NTP Server • 341
Specifying the Sensor Type • 371
States of Managed Sensors • 229
Status Bar • 86
Step A. Determine User Accounts and Groups • 470
Step B. Configure User Groups on the AD Server • 471
Step by Step Flexible Cord Installation • 451
Step C. Configure LDAP Authentication on the PX Device • 472
Step D. Configure User Groups on the PX Device • 474
Strong Passwords • 355
Supported Web Browsers • xvi, 77
Supported Wireless LAN Configuration • xvi, 21
Switch LHX • 182, 192
Switch Outlets • 182, 192
Switching an Outlet • 159
Switching Multiple or All Outlets • 158
Syslog Message • 182, 189

T

Testing the Network Connectivity • 445
Testing the Server Connection • 153
The PX MIB • 270
The Yellow- or Red-Highlighted Reading • 89, 93, 94, 156, 157, 171, 172, 228, 255
Three-Digit Row • 66
Time Configuration Commands • 339
Tracing the Network Route • 248
Tracing the Route • 446
Truncated Data in the Web Interface • 504
Turning Off the Outlet(s) • 439
Turning On the Outlet(s) • 438
Turning the LHX On or Off • 251, 257
Two-Digit Row • xvi, 67

U

Unblocking a User • 134, 441
Unmanaging Environmental Sensors • 224, 232
Unpacking the Product and Components • 13
Updating the Asset Sensor Firmware • 261
Updating the PX Firmware • 29, 258
Uppercase Character Requirement • 357
USB Wireless LAN Adapters • xvi, 20, 21
User Blocking • 354
User Configuration Commands • 404
User Management • 119
Using an X Cable • xvi, 56
Using SNMP • 259, 263
Using the CLI Command • xvi, 442, 468
Using the Command Line Interface • xvi, 105, 227, 273, 468
Using the PDU • 61
Using the Reset Button • 467
Using the Web Interface • 22, 77, 457

V

Viewing Connected Users • 216
Viewing Details • 255
Viewing Firmware Update History • 260
Viewing Sensor Data • 228
Viewing the Communication Log • 87, 249
Viewing the Dashboard • 93
Viewing the Local Event Log • 215
Viewing the Summary • 254, 256
Viewing the Webcam Snapshots or Videos • 59, 243

W

Warning Icon • 88
Webcam Management • 242
What is Assertion Timeout? • 174, 175, 176, 177, 178, 179, 225, 380, 386, 393, 399, 404
What is Deassertion Hysteresis? • 173, 174, 175, 176, 177, 178, 215, 225, 254, 379, 385, 392, 398, 403
What's New in the PX User Guide • xvi
Wired Network Settings • 99
Wireless Configuration • 280
Wireless Network Settings • 100
Wiring of 3-Phase In-Line Monitors • 449, 451
With HyperTerminal • 274, 441
With SSH or Telnet • 275

Z

Zero U Products • 4

U.S./Canada/Latin America

Monday - Friday
8 a.m. - 6 p.m. ET
Phone: 800-724-8090 or 732-764-8886
For CommandCenter NOC: Press 6, then Press 1
For CommandCenter Secure Gateway: Press 6, then Press 2
Fax: 732-764-8887
Email for CommandCenter NOC: tech-ccnoc@raritan.com
Email for all other products: tech@raritan.com

China

Beijing
Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-10-88091890

Shanghai
Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-21-5425-2499

GuangZhou
Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +86-20-8755-5561

India

Monday - Friday
9 a.m. - 6 p.m. local time
Phone: +91-124-410-7881

Japan

Monday - Friday
9:30 a.m. - 5:30 p.m. local time
Phone: +81-3-3523-5991
Email: support.japan@raritan.com

Europe

Europe
Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +31-10-2844040
Email: tech.europe@raritan.com

United Kingdom
Monday - Friday
8:30 a.m. to 5 p.m. GMT
Phone +44(0)20-7090-1390

France
Monday - Friday
8:30 a.m. - 5 p.m. GMT+1 CET
Phone: +33-1-47-56-20-39

Germany
Monday - Friday
8:30 a.m. - 5:30 p.m. GMT+1 CET
Phone: +49-20-17-47-98-0
Email: rg-support@raritan.com

Melbourne, Australia

Monday - Friday
9:00 a.m. - 6 p.m. local time
Phone: +61-3-9866-6887

Taiwan

Monday - Friday
9 a.m. - 6 p.m. GMT -5 Standard -4 Daylight
Phone: +886-2-8919-1333
Email: support.apac@raritan.com